

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10154193 A

(43) Date of publication of application: 09 . 06 . 98

(51) Int. Cl
G06F 19/00
G06K 17/00
G07F 19/00
G07F 7/08

(21) Application number: 09252048

(22) Date of filing: 17 . 09 . 97

(30) Priority: 30 . 09 . 96 JP 08258041

(71) Applicant: NTT DATA TSUSHIN KK

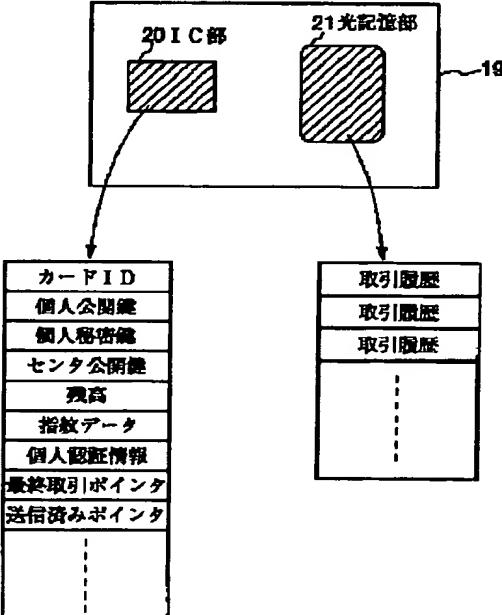
(72) Inventor: SATO SATORU
KITADA TOYOHIRO
TAKAGI TAKASHI
IIDA TOSHIHIDE

(54) ELECTRONIC MONEY SYSTEM AND
RECORDING MEDIUM

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent the forgery, etc., of money data and also to easily detect an illegal transaction.

SOLUTION: In a system in which electronic money is transacted by using an electronic money card 19, what is provided with an IC part 20 and an optical storage part 21 is used as the card 19. The part 21 records information that specifies the card 19, the balance, the fingerprint data of an owner and information that accesses a write once storage part 21, and the part 21 records the history of transactions which are performed by using the card 19. The fingerprint data that is registered on the card 19 of a remitter is added to the transaction history of an electronic money between electronic money cards, and virtually the same transaction history is recorded on the electronic money cards of a remitter and a remittee. The parts where illegality occurs and the amount of a sum are detected by tracking the transaction history.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-154193

(43)公開日 平成10年(1998)6月9日

(51)Int.Cl.⁶
G 0 6 F 19/00
G 0 6 K 17/00

G 0 7 F 19/00
7/08

識別記号

F I
G 0 6 F 15/30 3 6 0
G 0 6 K 17/00 L
S
G 0 6 F 15/30 3 5 0 A
G 0 7 D 9/00 4 7 6

審査請求 未請求 請求項の数18 OL (全27頁) 最終頁に続く

(21)出願番号 特願平9-252048
(22)出願日 平成9年(1997)9月17日
(31)優先権主張番号 特願平8-258041
(32)優先日 平8(1996)9月30日
(33)優先権主張国 日本 (JP)

(71)出願人 000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目3番3号
(72)発明者 佐藤 哲
東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内
(72)発明者 北田 豊浩
東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内
(72)発明者 高木 孝
東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内
(74)代理人 弁理士 木村 満

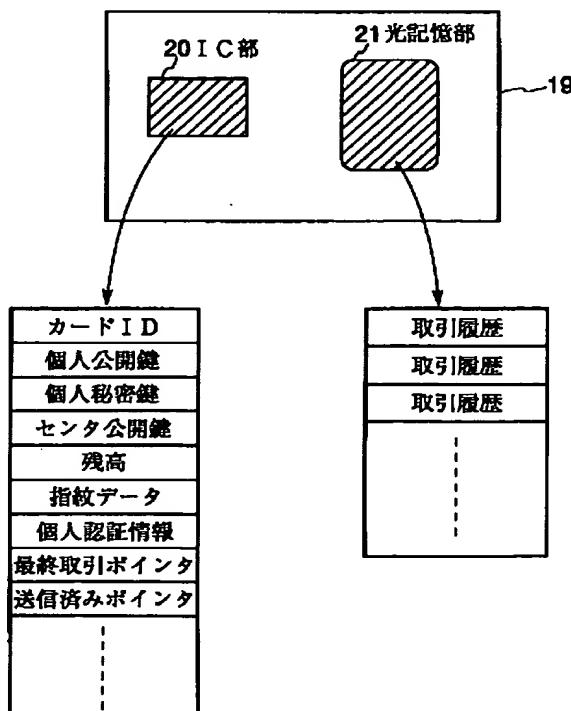
最終頁に続く

(54)【発明の名称】 電子マネーシステム及び記録媒体

(57)【要約】

【課題】 金銭データの偽造等を防止し、不正な取引を容易に検出することを可能とする電子マネーシステムを提供することを目的とする。

【解決手段】 電子マネーカード19を用いて電子マネーを取引するシステムにおいて、電子マネーカード19として、I C部20と光記憶部21とを備えるものを使用する。I C部20には、電子マネーカード19を特定するための情報、残高、所持者の指紋データ、追記型記憶部21をアクセスするための情報を記録し、光記憶部21には、電子マネーカード19を用いて行われた取引の履歴を記録する。電子マネーカード間の電子マネーの取引履歴には、送金元の電子マネーカード19に登録されている指紋データを付与し、送金元と送金先の電子マネーカードに実質的に同一の取引履歴を記録する。取引履歴を追跡することにより、不正の発生箇所、額等を検出できる。



【特許請求の範囲】

【請求項1】金銭的価値に関する電子マネーを格納する電子マネーカードと、該電子マネーカードを処理するための端末とを備え、前記電子マネーカード間で電子マネーを取引する電子マネーシステムであって、各前記電子マネーカードは、電子マネーの取引の履歴を示す取引履歴情報を記憶するための追記型記憶部を備え、前記端末は、取引元の前記電子マネーカードと取引先の前記電子マネーカードと取引金額を指示する手段と、前記取引元の電子マネーカードと前記取引先の電子マネーカードの前記追記型記憶部に今回の取引内容と操作者の身体的情報を含む取引履歴情報を追記する手段と、を備える、ことを特徴とする電子マネーシステム。

【請求項2】1回の取引について、前記取引元と取引先の前記電子マネーカードの前記追記型記憶部に記録される取引履歴情報は、実質的に同一の情報である、ことを特徴とする請求項1に記載の電子マネーシステム。

【請求項3】前記取引履歴情報は、取引金額と取引元の前記電子マネーカードの所有者の身体的情報を含む、ことを特徴とする請求項1又は2に記載の電子マネーシステム。

【請求項4】各前記電子マネーカードは、所有者の身体的情報を記憶したIC部を備え、前記端末は、取引元と取引先の前記電子マネーカードの前記追記型記録部に前記取引元の前記電子マネーカードの前記IC部から読み出した身体的情報を含む取引履歴情報を追記する、ことを特徴とする請求項1、2又は3に記載の電子マネーシステム。

【請求項5】前記端末は、操作者の身体的情報を読み取る読み取り装置とを備え、取引元と取引先の前記電子マネーカードの前記追記型記録部に前記読み取り装置により読み取った身体的情報を含む取引履歴情報を追記する、ことを特徴とする請求項1乃至4のいずれか1項に記載の電子マネーシステム。

【請求項6】前記端末は、取引元の前記電子マネーカードの前記追記型記録部に、譲渡金額と、前記取引元の前記電子マネーカードの操作者の身体的情報を含む取引履歴情報を追記し、取引先の前記電子マネーカードの前記追記型記録部に、譲受金額と、前記取引元の前記電子マネーカードの操作者の身体的情報を含む取引履歴情報を追記する、ことを特徴とする請求項1乃至5のいずれか1項に記載の電子マネーシステム。

【請求項7】前記電子マネーシステムは、各前記端末での電子マネーの取引を制御するためのコンピュータを備え、

該コンピュータは、前記電子マネーカードによる電子マネーの取引の取引履歴を記憶する取引履歴記憶手段を備える、ことを特徴とする請求項6に記載の電子マネーシステム。

【請求項8】前記電子マネーカードは、所有者の身体的情報を記憶しており、前記端末は、操作者の身体的情報を取得する取得手段と、前記電子マネーカードから前記身体的情報を読み出す読み出手段と、前記取得手段により取得された身体的情報とを比較し、実質的に一致するか否かを判別する判別手段と、前記判別手段が実質的に一致すると判断した時に、該端末を介した電子マネーの取引を可能とし、前記判別手段が実質的に一致しないと判断した時に、該端末を介した電子マネーの取引を禁止する取引制御手段と、を備える、

ことを特徴とする請求項1乃至7のいずれか1項に記載の電子マネーシステム。

【請求項9】前記身体的情報は、指紋、声紋、顔の画像、網膜パターンに関する情報のいずれかを含む、ことを特徴とする請求項1乃至8のいずれか1項に記載の電子マネーシステム。

【請求項10】前記電子マネーカードの前記追記型記憶部は、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成されている、ことを特徴とする請求項1乃至9のいずれか1項に記載の電子マネーシステム。

【請求項11】金銭的価値を有する電子マネーを格納する電子マネーカードを用いて電子マネーを取引する電子マネーシステムであって、

送金元の前記電子マネーカードと送金先の前記電子マネーカードと取引金額を入力する取引データ入力手段と、前記取引データ入力手段による入力に従って、前記送金元の前記電子マネーカードの残高を前記取引金額分減額し、前記送金先の前記電子マネーカードの残高を前記取引金額分増額する残高処理手段と、今回の取引の内容を示すと共に取引者を特定する個人特定情報を含む取引履歴情報を前記送金元と送金先の前記電子マネーカードに記録する取引履歴記録手段と、を備えることを特徴とする電子マネーシステム。

【請求項12】前記電子マネーカードは、所有者の個人特定情報を記憶しており、

前記取引履歴記録手段は、送金元の前記電子マネーカードから前記個人特定情報を読み出す読み出手段と、前記読み出手段により読み出された個人特定情報を取引履歴情報の一部として前記送金元と送金先の前記電子マネーカードに記録する手段と、を備えることを特徴とする請求項11に記載の電子マネーシステム。

【請求項13】送金元の前記電子マネーカードの保持者の前記個人特定情報を取得する取得手段と、前記取得手

段により取得された個人特定情報を取引履歴情報の一部として前記送金元と送金先の前記電子マネーカードに記録する手段と、を備えることを特徴とする請求項11に記載の電子マネーシステム。

【請求項14】前記電子マネーカードは追記型記憶部を備え、

前記取引履歴記録手段は前記送金元と送金先の前記電子マネーカードの前記追記型記憶部に前記取引履歴を記録する、

ことを特徴とする請求項11、12又は13に記載の電子マネーシステム。

【請求項15】金銭的価値を有する電子マネーを格納する電子マネーカードと、電子マネーカードを処理する複数の端末と、該複数の端末を処理するコンピュータを備え、電子マネーを取引する電子マネーシステムであつて、

各前記端末は、取引の内容を入力する入力手段と、取引者を特定する個人特定情報を取得する取得手段と、前記入力手段により入力された取引の内容と前記個人特定情報に基づいて、取引の内容と個人特定情報を含む取引要求電文を生成し、前記コンピュータに送信する手段と、前記コンピュータからの指示電文が取引の許可を指示する時に、送金元の前記電子マネーカードの残高を所定金額分減額し、送金先の前記電子マネーカードの残高を前記所定金額分増額する残高処理手段と、を備え、

前記コンピュータは、前記端末からの前記取引要求電文を受信し、該取引要求電文に基づいて、取引を許容するか否かを判別し、判別結果を表す前記指示電文を該端末に送信する、

ことを特徴とする電子マネーシステム。

【請求項16】コンピュータを、金銭的価値を有する電子マネーを格納する電子マネーカードを処理するための電子マネー端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であつて、該コンピュータを、取引元の前記電子マネーカードと取引先の前記電子マネーカードと取引金額を指示する手段、前記取引元の電子マネーカードと前記取引先の電子マネーカードの追記型記憶部に今回の取引内容と操作者の身体的情報を含む取引履歴情報を追記する手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項17】コンピュータを、金銭的価値を有する電子マネーを格納する電子マネーカードを処理する電子マネー端末として機能させるプログラムを記録するコンピュータ読み取り可能な記録媒体であつて、

該コンピュータを、送金元の前記電子マネーカードと送金先の前記電子マネーカードと取引金額を入力する取引データ入力手段、前記取引データ入力手段による入力に従って、前記送金元の前記電子マネーカードの残高を前記取引金額分減額し、前記送金先の前記電子マネーカー

ドの残高を前記取引金額分増額する残高処理手段、今回の取引の内容を示すと共に取引者を特定する個人特定情報を含む取引履歴情報を前記送金元と送金先の前記電子マネーカードに記録する取引履歴記録手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項18】コンピュータを、金銭的価値を有する電子マネーを格納する電子マネーカードを処理する複数の端末と、該複数の端末を処理するセンタと、を備えるシステムにおける前記端末として機能させるプログラムを記録するコンピュータ読み取り可能な記録媒体であつて、

該コンピュータを、取引の内容を入力する入力手段、取引者を特定する個人特定情報を取得する取得手段、前記入力手段により入力された取引の内容と前記個人特定情報に基づいて、取引の内容と個人特定情報を含む取引要求電文を生成し、前記センタに送信する送信手段、前記取引要求電文に応答して前記センタから返送された指示電文が取引の許可を指示する時に、送金元の前記電子マネーカードの残高を所定金額分減額し、送金先の前記電子マネーカードの残高を前記所定金額分増額する残高処理手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、金銭的情報である電子マネーを取引する電子マネーシステムに関する。

【0002】

【従来の技術】貨幣的価値を有する金銭データを用いて電子的な決済を可能とする電子マネーシステムが例えば、特公平7-111723等に開示されている。

【0003】

【発明が解決しようとする課題】電子マネーシステムでは、権限を有していない者の使用、金銭データのコピー、偽造等を有効に防止する必要がある。また、偽造等された金銭データの使用を発見した場合には、その流通経路を追跡し、不正元・偽造元等を発見できることが望ましい。しかし、このような要請を満たす電子マネーシステムは、未だに、提案されていない。

【0004】本発明は、上記実状に鑑みてなされたもので、金銭データの偽造等を有効に防止することができる電子マネーシステムを提供することを目的とする。また、本発明は、不正な取引を容易に検出し、その追跡性に優れた電子マネーシステムを提供することを目的とする。

【0005】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点に係る電子マネーシステムは、金銭的価値に関する電子マネーを格納する電子マネーカードと、該電子マネーカードを処理するための端末

とを備え、前記電子マネーカード間で電子マネーを取引する電子マネーシステムであって、各前記電子マネーカードは、電子マネーの取引の履歴を示す取引履歴情報を記憶するための追記型記憶部を備え、前記端末は、取引元の前記電子マネーカードと取引先の前記電子マネーカードと取引金額を指示する手段と、前記取引元の電子マネーカードと前記取引先の電子マネーカードの前記追記型記憶部に今回の取引内容と操作者の身体的情報を含む取引履歴情報を追記する手段と、を備える、ことを特徴とする。

【0006】このような構成によれば、電子マネーカードを用いて電子マネーを送受した際に、その履歴が追記型記録部に記録される。異常が発生した場合に、この追記型記録部の記録内容を検証することにより、不正行為等を容易に検出することができる。しかも、取引履歴が、指紋等の身体的情報を含んでるので、その信頼性を高めることができる。また、偽造等が困難になる。

【0007】1回の取引について、前記取引元と取引先の前記電子マネーカードの前記追記型記憶部に記録される取引履歴情報は、実質的に同一の情報としてもよい。このようにすれば、後日、情報を突き合わせる際の処理が容易になる。

【0008】前記取引履歴情報は、例えば、取引金額と取引元の前記電子マネーカードの所持者の身体的情情報を含む。

【0009】各前記電子マネーカードは所有者の身体的情情報を記憶したIC部を備え、前記端末は、取引元と取引先の前記電子マネーカードの前記追記型記録部に前記取引元の前記電子マネーカードの前記IC部から読み出した身体的情情報を含む取引履歴情報を追記するように構成してもよい。この構成によれば、身体的情報が予め電子マネーカードのIC部に登録されているので、処理を高速化することができる。また、電子マネーカードの保持者の正当性のチェック等にも利用できる。

【0010】前記端末は、例えば、操作者の身体的情情報を読み取る読み取り装置を備え、取引元と取引先の前記電子マネーカードの前記追記型記録部に前記読み取り装置により読み取った身体的情情報を含む取引履歴情報を追記するように構成してもよい。この構成によれば、実際に読み取った操作者の身体的情情報を取引履歴として記録するので、追跡性がより優れたものとなる。

【0011】取引元の電子マネーカードに記録される取引履歴情報は、例えば、譲渡金額と取引元の電子マネーカードの操作者の身体的情情報を含み、取引先の電子マネーカードに登録される取引履歴情報は、譲受金額と取引元の電子マネーカードの操作者の身体的情情報を含む。このような構成とすることにより、お金の流れに沿って、身体的情報が移動することになり、取引元の身体的情報を取引履歴情報に含めることにより、その取引の信頼性を高め、追跡性を高めることができる。

【0012】前記電子マネーシステムは、各前記端末での電子マネーの取引を制御するためのコンピュータを配置し、該コンピュータに、前記電子マネーカードによる電子マネーの取引の取引履歴を記憶する取引履歴記憶手段を配置してもよい。この構成により、電子マネーカードに記録された取引履歴との突き合わせが可能となると共に追跡性をより高めることができる。

【0013】前記電子マネーカードに、所有者の身体的情情報を予め記憶させておき、前記端末は、操作者の身体的情情報を取得する取得手段と、前記電子マネーカードから前記身体的情情報を読み出す読み出手段と、前記取得手段により取得された身体的情報とを比較し、実質的に一致するか否かを判別する判別手段と、前記判別手段が実質的に一致すると判断した時に、該端末を介した電子マネーの取引を可能とし、前記判別手段が実質的に一致しないと判断した時に、該端末を介した電子マネーの取引を禁止する取引制御手段と、を備えるように構成してもよい。この構成によれば、取引の際の操作者の正当性をその身体的情報に基づいて判別することができる。

【0014】前記身体的情報は、例えば、指紋、声紋、顔の画像、網膜パターンに関する情報等である。また、前記電子マネーカードの前記追記型記憶部は、例えば、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成される。なお、電子マネーカードは、実体として電子マネーの機能を有していればよく、その形状は、箱、円盤、ノート、手帳等、任意である。

【0015】この発明の第2の観点にかかる電子マネーシステムは、金銭的価値を有する電子マネーを格納する電子マネーカードを用いて電子マネーを取引する電子マネーシステムであって、送金元の前記電子マネーカードと送金先の前記電子マネーカードと取引金額を入力する取引データ入力手段と、前記取引データ入力手段による入力に従って、前記送金元の前記電子マネーカードの残高を前記取引金額分減額し、前記送金先の前記電子マネーカードの残高を前記取引金額分増額する残高処理手段と、今回の取引の内容を示すと共に取引者を特定する個人特定情報を含む取引履歴情報を前記送金元と送金先の前記電子マネーカードに記録する取引履歴記録手段と、を備えることを特徴とする。

【0016】この構成によれば、取引履歴情報が電子マネーカードに記録される。従って、取引履歴情報をチェックすることにより、不正行為等を検出し易くなる。しかも、取引履歴情報が、指紋等の身体的情情報を含んでるので、その信頼性を高めることができる。また、偽造等が困難になる。

【0017】前記電子マネーカードに所有者の個人特定情報を記憶させ、前記取引履歴記録手段は、送金元の前記電子マネーカードから前記個人特定情報を読み出す読み出手段と、前記読み出手段により読み出された個人特定情

報を取り履歴情報の一部として前記送金元と送金先の前記電子マネーカードに記録する手段と、を備えるように構成してもよい。この構成によれば、個人特定情報が電子マネーカードに登録されているので、処理を高速化することができる。また、電子マネーカードの保持者の正当性のチェック等にも利用できる。

【0018】また、端末に、送金元の前記電子マネーカードの保持者の前記個人特定情報を取得する取得手段と、前記取得手段により取得された個人特定情報を取引履歴情報の一部として前記送金元と送金先の前記電子マネーカードに記録する手段を配置してもよい。この構成によれば、取得した個人特定情報を取引履歴の一部として記録するので、追跡性がより優れたものとなる。

【0019】取引履歴は、前記送金元と送金先の前記電子マネーカードの前記追記型記憶部に記録することが望ましい。

【0020】この発明の第3の観点にかかる電子マネーシステムは、金銭的価値を有する電子マネーを格納する電子マネーカードと、電子マネーカードを処理する複数の端末と、該複数の端末を処理するコンピュータを備え、電子マネーを取引する電子マネーシステムであって、各前記端末は、取引の内容を入力する入力手段と、取引者を特定する個人特定情報を取得する取得手段と、前記入力手段により入力された取引の内容と前記個人特定情報に基づいて、取引の内容と個人特定情報を含む取引要求電文を生成し、前記コンピュータに送信する手段と、前記コンピュータからの指示電文が取引の許可を指示する時に、送金元の前記電子マネーカードの残高を所定金額分減額し、送金先の前記電子マネーカードの残高を前記所定金額分増額する残高処理手段と、を備え、前記コンピュータは、前記端末からの前記取引要求電文を受信し、該取引要求電文に基づいて、取引を許容するか否かを判別し、判別結果を表す前記指示電文を該端末に送信することを特徴とする。

【0021】この構成によれば、取引要求電文に個人特定情報を含む。従って、この個人特定情報から正当な操作者による操作であるかを判別し、取引を許可するか否かを判断することができる。

【0022】この発明の第4の観点にかかる記録媒体は、コンピュータを、金銭的価値を有する電子マネーを格納する電子マネーカードを処理するための電子マネー端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、取引元の前記電子マネーカードと取引先の前記電子マネーカードと取引金額を指示する手段、前記取引元の電子マネーカードと前記取引先の電子マネーカードの追記型記憶部に今回の取引内容と操作者の身体的情報を含む取引履歴情報を追記する手段、として機能させるためのプログラムを記録する。

【0023】この発明の第5の観点にかかる記録媒体

は、コンピュータを、金銭的価値を有する電子マネーを格納する電子マネーカードを処理する電子マネー端末として機能させるプログラムを記録するコンピュータ読み取り可能な記録媒体であって、該コンピュータを、送金元の前記電子マネーカードと送金先の前記電子マネーカードと取引金額を入力する取引データ入力手段、前記取引データ入力手段による入力に従って、前記送金元の前記電子マネーカードの残高を前記取引金額分減額し、前記送金先の前記電子マネーカードの残高を前記取引金額分増額する残高処理手段、今回の取引の内容を示すと共に取引者を特定する個人特定情報を含む取引履歴情報を前記送金元と送金先の前記電子マネーカードに記録する取引履歴記録手段、として機能させるためのプログラムを記録する。

【0024】この発明の第6の観点にかかる記録媒体は、コンピュータを、金銭的価値を有する電子マネーを格納する電子マネーカードを処理する複数の端末と、該複数の端末を処理するセンタと、を備えるシステムにおける前記端末として機能させるプログラムを記録するコンピュータ読み取り可能な記録媒体であって、該コンピュータを、取引の内容を入力する入力手段、取引者を特定する個人特定情報を取得する取得手段、前記入力手段により入力された取引の内容と前記個人特定情報に基づいて、取引の内容と個人特定情報を含む取引要求電文を生成し、前記センタに送信する送信手段、前記取引要求電文に応答して前記センタから返送された指示電文が取引の許可を指示する時に、送金元の前記電子マネーカードの残高を所定金額分減額し、送金先の前記電子マネーカードの残高を前記所定金額分増額する残高処理手段、として機能させるためのプログラムを記録する。

【0025】

【発明の実施の形態】以下、この発明の実施の形態にかかる電子マネーシステムを図面を参照して説明する。この電子マネーシステムは、図1に示すように、センタ10に配置されている認証局11及び電子マネーサーバ13と、電子マネー端末（取引装置）15と、銀行センタ17と、電子マネーカード19と、より構成される。

【0026】センタ10は、この電子マネーシステム全体の動作、電子マネーの流通を制御（管理）するコンピュータシステムである。センタ10の認証局11は、この電子マネーシステムにおける利用者等に対して認証情報を生成する。認証局11は、認証を行う際、利用者が登録されていることをチェックするため、このシステムにおいて使用される全ての電子マネーカード19のカードID及び公開鍵及び電子マネーカード19の所有者の指紋データを記憶する。

【0027】認証局11は、一対のセンタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、記憶する。認証局11は、電子マネーサーバ13にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ10内で共有化

する。また、認証局11は、センタ公開鍵Ck2を各電子マネー端末15等に電子マネーサーバ13を介して予め配布する。また、認証局11は、後述する個人認証情報を生成するための署名鍵Skと、その署名鍵Skによってなされた署名、即ち、個人認証情報を確認するための検査鍵Ekとを生成、記憶し、検査鍵Ekを各電子マネー端末15に予め配布しておく。

【0028】電子マネーサーバ13は、図2、図3に示すように、各電子マネーカード19が保持する電子マネーの残高を示す残高テーブル、使用不可になった電子マネーカード19のカードIDのリスト（事故カードリスト）、使用不可になった電子マネー端末15の端末IDのリスト（事故端末リスト）、電子マネーの取引の履歴のリスト（取引履歴テーブル）を記憶する。

【0029】電子マネーサーバ13は、これらの記憶データを用いて、認証局11への認証要求、銀行センタ17への振替要求、各電子マネーカード19及び電子マネー端末15及び電子マネーの取引の制御・管理等を行う。

【0030】電子マネー端末15は、利用者が電子マネーカード19を挿入又は装着し、所定の操作をすることにより、電子マネーの取引をするための端末である。電子マネー端末15には、電子マネーを電子マネーカード19に補充（チャージ）するためのチャージ端末（ATM等）、電子マネーカード相互間の電子マネーの授受を処理する端末、店舗等に配置され、物品やサービスの売り上げ金額に相当する電子マネーを受領するPOS端末、自動販売機等がある。1つの端末が電子マネーに関する複数の機能、例えば、ATM機能とPOS機能を備えている場合もある。

【0031】各電子マネー端末15は、記憶部30と、入力部31と、表示部32と、カード処理部33とを備える。

【0032】記憶部30は、その電子マネー端末15に付与された端末ID、前述の認証局11より供給された個人認証情報確認用の検査鍵Ek及びセンタ公開鍵Ck2、一対の端末秘密鍵Tk1と端末公開鍵Tk2とセンタ10とのオフライン時の電子マネーの取引履歴等を格納する。

【0033】入力部31は、電子マネー取引の指示を入力する。表示部32は、処理メニュー、メッセージ等を表示する。カード処理部33は、電子マネーカード19を受け付ける挿入口と、電子マネーカード19のIC部20をアクセスするためのICリード/ライト部と、光記憶部21をアクセスするための光記憶リード/ライト部とを備える。

【0034】図4(A)にATM型の電子マネー端末15の例を示す。この電子マネー端末15の入力部31と表示部32は、タッチパネル34から構成され、カード処理部33は、電子マネーカード19が挿入されるカ-

ド挿入口35Aと35Bを備える。カード挿入口35Aは、通常の処理と電子マネーの譲渡の際の譲渡元のカードが挿入される。カード挿入口35Bは、電子マネーの譲渡の際の譲渡先のカードが挿入される。

【0035】図4(B)にPOS型の電子マネー端末の例を示す。この電子マネー端末15の入力部31は、電子マネーの取引の指示等と共に売り上げ金額などを入力するためのキーボード31Aとバーコードリーダ31B等を含む。また、表示部32は、電子マネー取引のためメッセージ等と共に売り上げ金額などを表示し、顧客用の表示部32Aと操作者用の表示部32Bを備える。また、カード処理部33はカード挿入口35を備える。さらに、POS用に金銭ドロア36等も配置されている。

【0036】銀行センタ17は、電子マネーカード19の利用者（保有者）の口座である決済口座と銀行が保有する電子マネーの運用口座である別段口座を備え、これらの口座の入出金処理を行う。例えば、銀行センタ17は、センタ10からの指示に応じて電子マネーカード19に対応する決済口座から別段口座への振り替え及び別段口座から決済口座への振り替えを行う。この振り替え処理を行うため、銀行センタ17は、各電子マネーカード19に付与されているカードIDと各電子マネーカード19の利用者（保有者）の決済口座の口座番号を対応させる口座テーブルを図5に示すように記憶する。

【0037】電子マネーカード19は、図6に示すように、IC部（ICチップ）20と光記憶部21を備える光ICハイブリッドカードから構成される。IC部20は制御回路とメモリ回路を内蔵する。このメモリ回路は、図6に示すように、動作プログラムの他に、カードID、個人秘密鍵Pk1、個人公開鍵Pk2、電子マネーの残高、後述するオンライン取引用の個人認証情報、この電子マネーカード19の所有者の指紋データ等を記憶する。この指紋データは、例えば、指紋読み取り機で取得した指紋の画像データをフーリエ変換し、変換後のデータから位相情報を抽出することにより得られた位相情報である。また、IC部20は、後述する光記憶部21に記憶される取引履歴のうち、最終的な取引履歴の位置を示す最終取引ポインタと、電子マネーサーバ13へ最後に送信した取引履歴の位置を示す送信済みポインタを記憶する。

【0038】光記憶部21は、例えば、光エネルギーが照射されることによりピット等が形成されてデータが書き込まれるタイプの書き換え不可能な追記型の記憶媒体等から構成され、電子マネーカード19で取り引きされた電子マネーの取引履歴を順次記憶する。

【0039】取引履歴を構成する項目としては、電子マネーの取引の種別を示す利用区分（チャージ（残高の補充）、支払、譲渡、換金等）、取引のために電子マネーカードが装着された電子マネー端末15の端末ID、電

子マネーカード19間の電子マネーの授受の場合には相手のカードID、利用年月日、取引金額、認証子（上記項目と個人秘密鍵Pk1を用いて作成した取引認証子、上記項目と取引相手（電子マネー端末15又は他の電子マネーカード19）の秘密鍵を用いて作成した取引認証子）、等がある。電子マネーカード19間で取引を行った場合には、取引履歴は、送金元の指紋データを含む。

【0040】このような構成を有する電子マネーシステムにおける基本的な処理には、（1）電子マネーチャージ処理（電子マネーカード19に記憶される残高の補充）、（2）電子マネー譲渡処理、（3）個人認証情報発行処理、（4）電子マネー支払処理、（5）突き合わせ処理、（6）電子マネー換金処理、がある。これらの処理について、以下順番に説明する。

【0041】（1）電子マネーチャージ処理
電子マネーチャージ処理を、利用者Aが、電子マネー端末15B（端末ID”T150”）を用いて、自己の電子マネーカード19A（カードID”C99”）に1万円分の電子マネーをチャージする場合を例に、図7を参照して説明する。

【0042】電子マネー端末15Bは、図8（A）に示す処理選択画面を表示しており、利用者Aは、表示部32に表示された処理メニューから「1）電子マネーのチャージ」を選択する。この選択に応答し、電子マネー端末15Bは、図8（B）に示すように、電子マネーカード19の挿入を促すメッセージを表示する。利用者Aは、表示に従って、電子マネーカード19Aを電子マネー端末15Bに挿入する。この挿入に応答し、電子マネー端末15Bは、図8（C）に示す金額入力画面を表示する。利用者Aは、チャージ金額として「1万円」を入力する。

【0043】電子マネー端末15Bは、この入力に応答し、取引区分（チャージ）と利用年月日と取引金額とから構成される取引情報と端末ID”T150”とを、カードIDと個人公開鍵Pk2を要求する要求信号と共に電子マネーカード19Aに送信する（L1）。

【0044】電子マネーカード19Aは、受信した端末ID”T150”と取引情報にカードID”C99”を加え、個人秘密鍵Pk1Aを用いて取引認証子（Pk1A（T150+取引情報+C99））を作成する。電子マネーカード19Aは、作成した取引認証子（Pk1A（T150+取引情報+C99））をカードID”C99”と個人公開鍵Pk2Aと共に電子マネー端末15Bに送信する（L2）。

【0045】電子マネー端末15Bは、カードID”C99”と記憶部30に記憶していた取引情報に端末IDを加え、端末秘密鍵Tk1Bを用いて取引認証子（Tk1B（T150+取引情報+C99））を作成する。電子マネー端末15Bは、作成した取引認証子（Tk1B（T150+取引情報+C99））と、端末公開鍵Tk2

Bと端末ID”T150”とを含み、1万円分の電子マネーのチャージを要求するチャージ要求電文と、電子マネーカード19AのカードID”C99”と、個人公開鍵Pk2Aと、取引認証子（Pk1A（T150+取引情報+C99））とを、電子マネーサーバ13に送信する（L3）。

【0046】電子マネーサーバ13は、受信した端末ID”T150”とカードID”C99”が、事故端末リスト及び事故カードリストに登録されているか否かを判別することにより、電子マネー端末15及び電子マネーカード19の不正使用をチェックする。

【0047】チェックの結果、電子マネーカード19A及び電子マネー端末15Bが事故カードと事故端末のいずれでもないと判別されたならば、電子マネーサーバ13は、個人公開鍵Pk2Aを用いて取引認証子を端末IDと取引情報とカードIDとに変換する。又、端末公開鍵Tk2Bを用いて取引認証子を端末IDと取引情報とカードIDとに変換する。次いで、取引認証子から変換された端末IDと取引情報とカードIDと、取引認証子から変換された端末IDと取引情報とカードIDとが完全に一致するか否かを判別する。これらが完全に一致した場合、電子マネーサーバ13は、この取引認証子と取引認証子は正しいと判別し、銀行センタ17へカードID”C99”の決済口座から銀行センタ17の別段口座へ1万円を移動するよう指示する出金電文を送信する（L4）。

【0048】電子マネーカード19Aと電子マネー端末15Bの両方又は一方が事故カード又は事故端末であると判別された場合、及び／又は、取引認証子と取引認証子から変換された端末IDと取引情報とカードIDとが互いに一致しない場合、電子マネーサーバ13は、電子マネー端末15Bにチャージできない旨のメッセージを送信すると共に、不正又は異常の検出を管理者に通知する。

【0049】銀行センタ17は、出金電文を受信すると、図5に示す口座テーブルを参照してカードID”C99”の決済口座の口座番号”30000001”を検索し、該当する口座番号の残高が、指示されたチャージ金額の1万円以上か否かを判別する。残高が1万円未満の場合は、銀行センタ17は、残高不足のためチャージできない旨の電文を電子マネーサーバ13に送信する。残高が1万円以上の場合は、銀行センタ17は、決済口座”30000001”から銀行センタ17の別段口座へ1万円を移動し、出金完了電文を電子マネーサーバ13に送信する（L5）。

【0050】電子マネーサーバ13は、銀行センタ17から出金完了電文を受信すると、電子マネーカード19AのカードIDと個人公開鍵Pk2Aに対して認証を要求する認証付与要求を、カードID”C99”と個人公開鍵Pk2Aと共に認証局11へ送信する（L6）。

【0051】認証局11は、自己が記憶している電子マネーカード19AのカードID及び個人公開鍵Pk2のリストに、受信したカードID"C99"と個人公開鍵Pk2Aが存在する（即ち、この電子マネーシステムに登録されている）ことをチェックする。カードID"C99"と個人公開鍵Pk2Aとが認証局11に登録されている場合、認証局11は、センタ秘密鍵Ck1を用いて、受信したカードID"C99"と個人公開鍵Pk2Aに対する認証情報{Ck1(C99+Pk2A)}を生成し、認証の完了を示す認証完了電文と共に電子マネーサーバ13に送信する（L7）。

【0052】電子マネーサーバ13は、認証完了電文を受信すると、利用区分"チャージ"、利用年月日、カードID"C99"、端末ID"T150"、チャージ金額"1万円"、取引認証子、取引先認証子、等により取引履歴を生成して図3に示すように記憶する。また、図2(A)に示す残高テーブルのカードID"C99"の残高を1万円加算する。さらに、生成した取引履歴に認証局11からの認証情報{Ck1(C99+Pk2A)}を付与して、チャージ完了電文と共に電子マネー端末15Bに送信する（L8）。

【0053】電子マネー端末15Bは、取引履歴に付与された認証情報{Ck1(C99+Pk2A)}をセンター公開鍵Ck2を用いて、カードID"C99"と個人公開鍵Pk2Aに変換し、その認証情報が正しいものであることを確認すると、受信した取引履歴を電子マネーカード19AのIC部20に送信する（L9）。IC部20は、受信した取引履歴に基づいて、自己が記憶している残高に1万円を加算する。また、電子マネー端末15Bは、IC部20から最終取引ポイントを読み出し、光記憶部21の最終取引ポイントが示す位置の次の位置に取引履歴を追記し、最終取引ポイント及び送信済みポイントを追記された取引履歴を示すように更新する。その後、端末15Bはチャージが完了した旨を表示部32に表示すると共に電子マネーカード19Aを排出する。このようして、各利用者は自己の電子マネーカード19Aに、電子マネーをチャージすることができる。

【0054】(2) 電子マネーの譲渡処理

次に、電子マネー譲渡処理の概要を図9を参照して説明する。電子マネーを譲渡（送金）する側を電子マネーカード19Aとし、譲渡を受ける（受金）側を電子マネーカード19Bとする。

【0055】図8に示す画面表示に従って、表示部32(タッチパネル34)に表示される処理メニューから「2)電子マネーの譲渡」が選択され、送金元の電子マネーカード19Aが挿入口35Aに送金先の電子マネーカード19Bが挿入口35Bにそれぞれ挿入され、電子マネーカード19Aから電子マネーカード19Bへの譲渡（送金）金額が入力される。

【0056】電子マネー端末15は、この入力に応答し

て、電子マネーカード19Aと電子マネーカード19Bに、取引区分（19Aから19Bへの譲渡）と利用年月日と取引金額とから構成される取引情報と端末IDと、カードIDと個人公開鍵の要求を示す要求信号をそれぞれ送信する（P41）。

【0057】電子マネーカード19Aは、要求信号に応答し、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Aを用いて、端末IDと取引情報と自己のカードIDに対する取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}を作成する。電子マネーカード19Aは、作成した取引認証子とカードIDと個人公開鍵Pk2Aと指紋データを電子マネー端末15に送信する（P42）。

【0058】また電子マネーカード19Bは、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Bを用いて、端末IDと取引情報と自己のカードIDに対する取引認証子{Pk1B(端末ID+取引情報+19BのカードID)}を作成する。電子マネーカード19Bは、作成した取引先認証子とカードIDと個人公開鍵Pk2Bとを電子マネー端末15に送信する（P42）。

【0059】電子マネー端末15は、電子マネーカード19Aから受信した取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}とカードIDと個人公開鍵Pk2Aと指紋データと、電子マネーカード19Bから受信した取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}とカードIDと個人公開鍵Pk2Bと、電子マネーカード19Aから電子マネーカード19Bに入力された金額（譲渡金額）を移動するよう指示する譲渡依頼電文とを、電子マネーサーバ13に送信する（P43）。なお、譲渡依頼電文は端末IDを含む。

【0060】電子マネーサーバ13は、受信した電子マネーカード19Aと電子マネーカード19BのカードID及び端末IDが事故カードIDリスト及び事故端末IDリストに登録されているか否かを判別する。

【0061】受信したカードID及び端末IDが、事故カードIDリスト及び事故端末IDリストに登録されていない場合、電子マネーサーバ13は、図2(A)に示す残高テーブルの電子マネーカード19Aの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末15に送信する。電子マネー端末15は、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【0062】残高が指示された譲渡金額以上の場合、電子マネーサーバ13は、電子マネーカード19Aの個人公開鍵Pk2Aを用いて取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}を端末IDと取引情報と電子マネーカード19AのカードIDとに変換する。又、電子マネーカード19Bの個人公開鍵Pk2Bを用いて取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}を端末IDと取引情報と電子マネーカード19BのカードIDとに変換する。

9 BのカードID) }を端末IDと取引情報とカードIDとに変換する。次に、変換した内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から変換された取引情報及び端末IDが一致しており、取引認証子から変換されたカードIDが譲渡元の電子マネーカード19AのカードIDに一致し、取引先認証子から変換したカードIDが譲渡先の電子マネーカード19BのカードIDに一致することをチェックする。全て一致すると判別された場合、残高テーブルの電子マネーカード19Aと電子マネーカード19Bの残高をそれぞれ更新する。

【0063】次に、電子マネーサーバ13は、電子マネーカード19AのカードIDと個人公開鍵Pk2Aと指紋データ、及び、電子マネーカード19BのカードID及び個人公開鍵Pk2Bを認証付与要求と共に認証局11に送信する(P44)。

【0064】認証局11は、認証付与要求に応答し、受信した電子マネーカード19AのカードID及び個人公開鍵Pk2Aと指紋データ、及び、電子マネーカード19BのカードID及び個人公開鍵Pk2Bが予め登録されているか否かをチェックする。これらが登録されていると判断された場合、それらに対してセンタ秘密鍵Ck1を用いて認証情報〔Ck1(19AのカードID+Pk2A)、〔Ck1(19BのカードID+Pk2B)〕をそれぞれ生成し、認証完了電文と共に電子マネーサーバ13に送信する(P45)。

【0065】電子マネーサーバ13は、認証完了電文に応答し、譲渡元(送金元)の電子マネーカード19Aの取引履歴と譲渡先(送金先)の電子マネーカード19Bの取引履歴を生成して、取引履歴テーブルに記憶する。また、電子マネーサーバ13は、残高テーブルの電子マネーカード19Aと19Bの残高をそれぞれ更新する。電子マネーカード19Aと19Bの取引履歴は、共に、利用区分として「譲渡」、「端末ID」、「利用年月日」、「譲渡元の指紋データとカードID」、「取引金額」、「認証子(取引認証子と取引先認証子)」とからなり、実質的に一致する。さらに、電子マネーサーバ13は認証情報を取引履歴に付与し、譲渡完了電文と共に電子マネー端末15に送信する(P46)。

【0066】電子マネー端末15は、譲渡完了電文に応答し、受信した認証情報〔Ck1(C99+Pk2A)〕をセンター公開鍵Ck2を用いて、カードID"C99"と個人公開鍵Pk2Aに変換し、〔Ck1(C05+Pk2B)〕をセンター公開鍵Ck2を用いて、カードID"C05"と個人公開鍵Pk2Bに変換し、その認証情報が正しいものであることを確認すると、受信した取引履歴を電子マネーカード19Aと電子マネーカード19Bへそれぞれ送信する(P47)。電子マネーカード19Aと19BのIC部20は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マ

ネーカード19AのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード19BのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【0067】さらに、電子マネーカード19A、19BのIC部20は、それぞれ、最終取引ポインタの値を電子マネー端末15に送信する。電子マネー端末15は、電子マネーカード19Aと19Bの光記憶部21の、最終取引ポインタの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポインタ及び送信済みポインタを、追記された取引履歴を示すように更新する。

【0068】この電子マネー譲渡処理を、利用者Aの電子マネーカード19A(カードID"C99")から利用者Bの電子マネーカード19B(カードID"C05")へ、電子マネー端末15C(端末ID"T150")を介して3万円分の電子マネーを譲渡する場合を例に図10を参照して説明する。

【0069】まず、利用者AとBは、図8に示す画面表示に従って、処理メニューから「3)電子マネーの譲渡」を選択し、電子マネーカード19Aを譲渡元カード挿入口35Aに挿入し、電子マネーカード19Bを譲渡先カード挿入口35Bに挿入し、譲渡金額の3万円を入力する。

【0070】この入力に応答して、電子マネー端末15Cは、電子マネーカード19Aと電子マネーカード19Bに、取引区分と利用年月日と取引金額とから構成される取引情報と端末ID"T150"と共に、カードIDと個人公開鍵の要求を示す要求信号をそれぞれ送信する(L41)。

【0071】電子マネーカード19Aは、要求信号に応答し、端末ID"T150"と取引情報に自己のカードID"C99"を加え、個人秘密鍵Pk1Aを用いて取引認証子〔Pk1A(T150+取引情報+C99)〕を作成し、その取引認証子をカードID"C99"と個人公開鍵Pk2Aと指紋データと共に電子マネー端末15Cに送信する(L42)。

【0072】また、電子マネーカード19Bは、要求信号に応答し、端末ID"T150"と取引情報に自己のカードID"C05"を加え、個人秘密鍵Pk1Bを用いて取引先認証子〔Pk1B(T150+取引情報+C05)〕を作成し、その取引先認証子をカードID"C05"と個人公開鍵Pk2Bと共に電子マネー端末15Cに送信する(L42)。

【0073】電子マネー端末15Cは、電子マネーカード19Aから受信したカードID"C99"と個人公開鍵Pk2Aと取引認証子〔Pk1A(T150+取引情報+C99)〕と指紋データと、電子マネーカード19Bから受信したカードID"C05"と個人公開鍵Pk2Bと取引先認証子〔Pk1B(T150+取引情報+C05)〕

5) } と、端末ID" T150" を含み、電子マネーカード19Aから電子マネーカード19Bへ3万円の電子マネーを移動するよう指示する譲渡依頼電文とを、電子マネーサーバ13に送信する (L43)。

【0074】電子マネーサーバ13は、受信した電子マネーカード19Aと電子マネーカード19BのカードID" C99"、" C05" 及び端末ID" T150" が事故カードID及び事故端末IDのリストに登録されているか否かをチェックする。カードID" C99"、" C05" 及び端末ID" T150" が、事故カード又は事故端末として登録されていないと判別された場合、電子マネーサーバ13は、譲渡元の電子マネーカード19Aの残高を残高テーブルを参照してチェックする。

【0075】残高が3万円未満ならば、電子マネーサーバ13は、残高不足の旨のメッセージを電子マネー端末15Cに送信する。残高が3万円以上ならば、電子マネーサーバ13は、個人公開鍵Pk2Aを用いて取引認証子{Pk1A (T150+取引情報+C99)}を端末IDと取引情報と電子マネーカード19AのカードIDとに変換する。又、個人公開鍵Pk2Bを用いて取引先認証子{Pk1B (T150+取引情報+C05)}を端末IDと取引情報とカードIDとに変換する。

【0076】統いて、これらの内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から変換した端末IDと取引情報とが互いに一致しており、取引認証子から変換されたカードIDが譲渡元の電子マネーカード19AのカードID" C99" に一致し、取引先認証子から変換されたカードIDが譲渡先の電子マネーカード19BのカードID" C05" に一致するか否かをチェックする。チェックの結果、取引認証子と取引先認証子が正しいと判別されたならば、電子マネーサーバ13は、残高テーブルにおけるカードID" C99" の残高を3万円だけ減算し、カードID" C05" の残高に3万円を加算する。次に電子マネーサーバ13は、電子マネーカード19AのカードID" C99" と個人公開鍵Pk2Aと指紋データと、電子マネーカード19BのカードID" C05" と個人公開鍵Pk2Bを認証局11に認証付与要求と共に送信する (L44)。

【0077】認証局11は、認証付与要求に応答し、自己が記憶するカードIDと公開鍵と指紋データのリストを参照することにより、受信した電子マネーカード19Aと電子マネーカード19BのカードID" C99"、" C05" 及び個人公開鍵Pk2A、Pk2B及び指紋データがこのシステムに登録されているか否かをチェックする。認証局11は、それらが登録されていることを確認すると、カードID" C99"、" C05" 及び個人公開鍵Pk2A、Pk2Bに対してセンタ秘密鍵Ck1を用いて電子マネーカード19Aの認証情報{Ck1 (C99+Pk2A)}と電子マネーカード19Bの認証情報{Ck1 (C05+Pk2B)}をそれぞれ生成し、認証完

了電文と共に電子マネーサーバ13に送信する (L45)。

【0078】電子マネーサーバ13は、認証完了電文と電子マネーカード19Aと電子マネーカード19Bの認証情報{Ck1 (C99+Pk2A)}と{Ck1 (C05+Pk2B)}を受信すると、図11(A)と(B)に示すように、譲渡元の電子マネーカード19Aの取引履歴と譲渡先の電子マネーカード19Bの取引履歴を生成し、取引履歴テーブルに記憶する。さらに、それらの取引履歴に認証局11からの認証情報を付与し、譲渡完了電文と共に電子マネー端末15Cに送信する (L46)。また、電子マネーサーバ13は、残高テーブルの電子マネーカード19Aと19Bの残高をそれぞれ更新する。

【0079】電子マネー端末15Cは、受信した認証情報{Ck1 (C99+Pk2A)}をセンター公開鍵Ck2を用いて、カードID" C99"と個人公開鍵Pk2Aに変換し、{Ck1 (C05+Pk2B)}をセンター公開鍵Ck2を用いて、カードID" C05"と個人公開鍵Pk2Bに変換し、それらが正しいことを確認すると、受信した取引履歴を電子マネーカード19Aと19BのIC部20にそれぞれ送信する (L47)。電子マネーカード19Aと19BのIC部20は、受信した取引履歴に基づいて記憶回路に記憶している残高を更新する。即ち、電子マネーカード19Aは残高を3万円減額し、電子マネーカード19Bは残高を3万円増額する。さらに、電子マネー端末15Cは、電子マネーカード19Aと19BのIC部20から最終取引ポインタの値を読み出し、電子マネーカード19Aと19Bの光記録部21の最終取引ポインタが値が示すアドレスの次のアドレスに、取引履歴をそれぞれ追記する。

【0080】さらに、端末15Cは、電子マネーカード19Aと19BのIC部20に記憶されている最終取引ポインタ及び送信済みポインタを追記された取引履歴を示すように更新する。

【0081】このような譲渡(送金)処理により、AさんからBさんに1000円、次に、BさんからCさんに3000円、さらに、CさんからAさんに2000円移動した場合に、各電子マネーカードの光記憶部21に登録される取引履歴の主要部の一例を図12に示す。

【0082】まず、AさんからBさんへの1000円の送金により、Aの電子マネーカードには、出金情報として、送金元であるAのカードIDと指紋データと金額「¥1000」が記録され、Bの電子マネーカードには、入金情報として、送金元であるAのカードIDと指紋データと金額「¥1000」が記録される。次に、BさんからCさんへの3000円の送金により、Bの電子マネーカードには、出金情報として、送金元であるBのカードIDと指紋データと金額「¥3000」が記録され、Cの電子マネーカードには、入金情報として、送金元であるBのカードIDと指紋データと金額「¥3000」

0」が記録される。さらに、CさんからAさんへの200円の送金により、Cの電子マネーカードには、出金情報として、送金元であるCのカードIDと指紋データと金額「¥2000」が記録され、Aの電子マネーカードには、入金情報として、送金元であるAのカードIDと指紋データと金額「¥2000」が記録される。

【0083】同様の取引履歴が、電子マネーサーバ13の各電子マネーカード用の取引履歴テーブルにも格納される。

【0084】なお、譲渡元の電子マネーカード19Aの残高のチェックは、「3) 電子マネーの譲渡」がメニューにより選択され、譲渡金額が入力されたときに電子マネー端末15が行うようにしてもよい。この場合、電子マネー端末15は、電子マネーカード19Aに残高要求を行う。

【0085】(3) 個人認証情報発行処理

次に、電子マネーカード19のIC部20に記憶される個人認証情報の発行処理(個人認証情報発行処理)について説明する。後述するオフラインによる電子マネー支払い処理において、電子マネーカード19は、この個人認証情報を電子マネー端末15に提示し、電子マネー端末15によりその個人認証情報の確認を受けることで、取引することが可能となる。個人認証情報は、電子マネーカード19のカードID及び個人公開鍵Pk2をもとに作成されるため、個人秘密鍵Pk1及び個人公開鍵Pk2が変更される度に取得される必要がある。

【0086】図13に個人認証情報発行処理の概要図を示す。まず、図8に示すように、表示部32に表示される処理メニューから「4) 個人認証情報の発行」が選択され、電子マネーカード19が電子マネー端末15Bに挿入する。電子マネー端末15は、この操作に応答し、電子マネーカード19AにカードIDと個人公開鍵の送信を要求する要求信号を送信する(L11)。

【0087】電子マネーカード19AのIC部20は、電子マネー端末15Bからの要求信号を受信すると、カードID" C99"と個人公開鍵Pk2Aを電子マネー端末15Bに送信する(L12)。電子マネー端末15Bは、受信したカードID" C99"と個人公開鍵Pk2Aを認証情報発行要求と共に電子マネーサーバ13に送信する(L13)。

【0088】電子マネーサーバ13は、受信したカードID" C99"と個人公開鍵Pk2Aとが、事故カードIDリスト及び事故端末IDリストに登録されているか否かを判別することにより、電子マネーカード19及び電子マネー端末15の不正使用をチェックする。不正使用と判別された場合、電子マネーサーバ13は、電子マネー端末15Bに個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末15Bは、このメッセージを表示する。

【0089】チェックの結果、電子マネーカード19A及び電子マネー端末15Bが使用可能ならば、カードID" C99"と個人公開鍵Pk2Aを個人認証情報発行要求と共に認証局11へ送信する(L14)。

【0090】認証局11は、電子マネーサーバ13から受信したカードID" C99"と個人公開鍵Pk2Aに署名鍵Skを用いてデジタル署名を施すことにより個人認証情報{Sk(C99+Pk2A)}を生成し、発行完了電文と共に電子マネーサーバ13に送信する(L15)。

【0091】電子マネーサーバ13は、認証局11からの個人認証情報{Sk(C99+Pk2A)}と発行完了電文を電子マネー端末15に送信する(L16)。電子マネー端末15Bは、電子マネーサーバ13から受信した個人認証情報を電子マネーカード19Aに送信する(L17)。電子マネーカード19AのIC部20は、電子マネー端末15Bから受信した個人認証情報を記憶する。

【0092】個人認証情報は、個人秘密鍵Pk1及び個人公開鍵Pk2が電子マネー端末15で変更された際に、自動的に該電子マネー端末15を介して取得されてもよい。

【0093】(4) 電子マネー支払い処理

電子マネー支払い処理を、例えば、利用者Aが、端末IDが" T150"の電子マネー端末15Bが設定された店舗において1万円の商品又はサービスを購入し、その支払いを電子マネーカード19A(カードID" C99")で行う場合を例に図14を参照して説明する。電子マネー端末15Bは、例えば、図4(B)に示すようなPOS端末、自動販売機、等の形態をとる。

【0094】まず、電子マネー端末15B(例えばPOS端末)の表示部32に金額" 1万円"が支払金額として表示され、利用者が電子マネーによる支払いを選択したとする。まず、利用者A又は店員が電子マネーカード19Aを電子マネー端末15Bに挿入する。

【0095】電子マネー端末15Bは、電子マネーカード19Aの挿入に応答して、取引区分と取引年月日と取引金額とから構成される取引情報と端末ID" T150"と、カードID" C99"と個人公開鍵Pk2Aと個人認証情報と残高の送信を要求する要求信号を電子マネーカード19Aに送信する(L21)。

【0096】電子マネーカード19Aは、受信した端末ID" T150"と取引情報にカードID" C99"を加え、個人秘密鍵Pk1Aを用いて取引認証子{Pk1A(T150+取引情報+C99)}を作成する。電子マネーカード19Aは、作成した取引認証子{Pk2A(T150+取引情報+C99)}と、カードID" C99"と、個人公開鍵Pk2Aと、個人認証情報{Sk(C99+Pk2A)}と、残高とを電子マネー端末15に送信する(L22)。

【0097】電子マネー端末15Bは、電子マネーカード19Aから、カードID”C99”と個人公開鍵Pk2Aと個人認証情報{Sk(カードID+Pk2A)}と残高と取引認証子{Pk1A(T150+取引情報+C99)}とを受信し、個人認証情報{Sk(C99+Pk2A)}を、予め記憶している検査鍵Ekを用いてカードIDと個人公開鍵Pk2Aに変換する。次に、個人認証情報から変換されたカードIDと個人公開鍵Pk2Aが、電子マネーカード19AのカードID”C99”と個人公開鍵Pk2Aと一致することを確認する。

【0098】次に、電子マネー端末15Bは、電子マネーカード19Aの残高が支払い金額（この場合1万円）以上か否かを判別する。残高が1万円以上ならば、電子マネー端末15Bは、端末ID”T150”と取引情報とカードID”C99”に対して端末秘密鍵Tk1を用いて取引認証子{Tk1(T150+取引情報+C99)}を生成する。さらに、端末ID”T150”と取引情報とカードID”C99”と取引認証子{Tk1(T150+取引情報+C99)}と取引認証子{Tk1(T150+取引情報+C99)}より取引履歴を構成し、支払い完了電文と共に電子マネーカード19Aへ送信する（L23）。また、取引履歴を自己の記憶部30にも記憶する。

【0099】電子マネーカード19AのIC部20は、電子マネー端末15Bから受信した取引履歴に基づいて、残高を1万円分減算すると共に最終取引ポインタの値を電子マネー端末15Bに送信する。電子マネー端末15Bは、光記録部21の最終取引ポインタが示すアドレスの次のアドレスに取引履歴を格納する。その後、IC部20に最終取引ポインタの値を次のアドレス位置を示すように更新する。ただし、送信済みポインタの値は更新しない。

【0100】一方、電子マネー端末15Bが、個人認証情報Sk(カードID+Pk2A)から変換されたカードIDと個人公開鍵Pk2Aが電子マネーカード19AのカードID”C99”と個人公開鍵Pk2Aと一致しないと判断した場合、電子マネー端末15Bは電子マネーカード19Aを不正カードと判別し、支払い不可の旨のメッセージを表示部32に表示すると共に、不正検出を電子マネーサーバ13に通知する。また、電子マネーカード19Aの残高が1万円未満の場合、電子マネー端末15Bは、残高不足のため支払い不可の旨のメッセージを表示部32に表示する。

【0101】電子マネー端末15Bは、記憶部30に記憶していた取引履歴を支払い処理終了後、電子マネーサーバ13に送信する。電子マネーサーバ13は取引履歴を受信すると、受信した取引履歴を図3に示すように、取引履歴テーブルに格納する。電子マネー端末15Bは、記憶部30に蓄積していた取引履歴の電子マネーサーバ13への送信完了後、送信済みの取引履歴を消去し

てもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【0102】(5) 突き合わせ処理

支払い処理等が実行されると、電子マネーカード19には、電子マネーサーバ13に対して未送信の取引履歴が発生する。これらの取引履歴は、オンラインで行われる処理（例えば、電子マネーのチャージ処理等）の実行時、その処理に先だって電子マネーサーバ13に送信される。電子マネーサーバ13は、電子マネーカード19から取引履歴を電子マネー端末15を介して受信すると、自己が記憶している取引履歴と突き合わせることにより、その正当性をチェックする。この突き合わせ処理の概要を図15を参照して説明する。

【0103】電子マネーカード19のIC部20は、電子マネー端末15からの信号を受信すると、受信した信号が指示する処理の内容を判別し、それがオンライン処理を指示しているか否かを判別する。受信信号がオンライン処理を指示している際には、IC部20は、他の処理を実行する前に、最終取引ポインタの値と送信済みポインタの値とが一致している否かを判別する。一致していないと判別した場合、IC部20は、割り込み信号と共に、送信済みポインタが示すポインタの次の位置から、最終取引ポインタが示す位置までの各アドレスに記憶されている取引履歴とカードIDと個人公開鍵を電子マネー端末15に送信する。

【0104】なお、最終取引ポインタと送信済みポインタとが一致する場合、未送信履歴が存在しないため、電子マネーカード19は、要求信号に応じた処理を続行する。

【0105】例えば、利用者Aが、電子マネーのチャージを指示し、電子マネーカード19Aを電子マネー端末15Bに挿入したとする。電子マネー端末15は、取引区分（チャージ）と利用年月日と取引金額とから構成される取引情報と端末IDとを、カードIDと個人公開鍵Pk2を要求する要求信号と共に電子マネーカード19AのIC部20に送信する。

【0106】IC部20は、取引情報から、オンライン処理が選択されたことを判別し、内部に記憶している最終取引ポインタと送信済みポインタとが一致するか否かを判別する。図16に示すように、送信済みポインタはアドレス”2”を指し、最終取引ポインタはアドレス”5”を示しているとすると、IC部20は、送信済みポインタが指しているアドレス”2”的次のアドレス”3”から最終取引ポインタが指しているアドレス”5”までの取引履歴R3～R5を割り込み信号とカードID”C99”と個人公開鍵Pk2Aと共に電子マネー端末15Bに送信する（L31）。電子マネー端末15Bは、受信した取引履歴R3～R5とカードIDと個人公開鍵Pk2Aを電子マネーサーバ13へ送信する（L3

2)。

【0107】電子マネーサーバ13は、受信したカードID”C99”と個人公開鍵Pk2Aを確認要求と共に認証局11に送信する(L33)。認証局11は、自分が記憶するカードIDと個人公開鍵のリストに、受信したカードIDと個人公開鍵Pk2Aが登録されていることを確認し、確認完了電文を電子マネーサーバ13に送信する(L34)。

【0108】電子マネーサーバ13は、確認完了電文を受信すると、取引履歴R3～R5と自己が記憶している取引履歴とを突き合わせる。即ち、アドレス”3”～”5”の取引履歴R3～R5が全て電子マネーサーバ13に記憶されている取引履歴と一致することをチェックする。チェックの結果、取引履歴R3～R5が電子マネーサーバ13に記憶されている取引履歴と一致するならば、電子マネーサーバ13は、図2(A)に示す残高テーブルのカードID”C99”的残高を更新し、電子マネー端末15Bに突き合わせ完了電文を送信する(L35)。電子マネー端末15Bは、受信した突き合わせ完了電文を電子マネーカード19Aに送信する(L36)。電子マネーカード19Aは、突き合わせ完了電文を受信すると、図16に示すように、IC部20に記憶している送信済みポイントを”2”から”5”に更新する。

【0109】その後、電子マネー端末15Bと電子マネーカード19Aは指示されている電子マネーチャージ処理を実行する。

【0110】上述した突き合わせ処理では、電子マネーカード19からの取引履歴と電子マネーサーバ13に記憶されている電子マネー端末15Bからの取引履歴を比較する。これにより、不正に生成された(例えば、取引金額が改竄された)取引履歴を容易に検出することができる。また、不正が検出された際、不正な電子マネーカード19の光記憶部21に記憶されている取引履歴を参照することにより、いつ、どこで、いくら使用されたか、等の使用履歴を知ることができる。

【0111】(6) 電子マネー換金処理

次に、電子マネーカード19に蓄積している電子マネーを換金する処理を、この電子マネー換金処理を、利用者Aが電子マネーカード19A(カードID”C99”)に記憶している電子マネーうち5万円を、電子マネー端末15B(端末ID”T150”)を用いて、銀行センタ17の自己の決済口座に振り替える場合を例に図17を参照して説明する。利用者Aは、表示部32に表示される処理メニューから「2)電子マネー換金」を選択し、電子マネーカード19Aを電子マネー端末15Bに装着し、換金金額「5万円」を入力部31に入力する。

【0112】この操作に応答して、電子マネー端末15Bは、電子マネーカード19Aに、取引区分と利用年月日と取引金額とから構成される取引情報と、端末ID”

T150”と、カードIDと個人公開鍵の送信を要求する要求信号と、を送信する(L51)。電子マネーカード19Aは、要求信号に応答し、受信した端末ID”T150”及び取引情報に自己のカードID”C99”を加え、個人秘密鍵Pk1Aを用いて取引認証子{Pk1A(T150+取引情報+C99)}を作成する。電子マネーカード19Aは、作成した取引認証子{Pk1A(T150+取引情報+C99)}とカードID”C99”と個人公開鍵Pk2Aを電子マネー端末15Bに送信する(L52)。

【0113】電子マネー端末15Bは、受信したカードID”C99”に取引情報と端末ID”T150”を加え、端末秘密鍵Tk1を用いて取引先認証子{Tk1B(T150+取引情報+C99)}を作成する。電子マネー端末15Bは、作成した取引先認証子{Tk1B(T150+取引情報+C99)}と、入力された換金金額を電子マネーカード19Aからその電子マネーカード19Aに対応する決済口座に振り替えることを指示し、端末公開鍵Tk2Bを含む換金要求と、電子マネーカード19AのカードID”C99”と、個人公開鍵Pk2Aと、取引認証子{Pk1A(T150+取引情報+C99)}とを電子マネーサーバ13へ送信する(L53)。

【0114】電子マネーサーバ13は、電子マネーカード19AのカードID”C99”及び端末ID”T150”が事故カードIDリスト及び事故端末IDリストに登録されているか否かチェックする。受信したカードID”C99”及び端末ID”T150”が、事故カードIDリスト及び事故端末IDリストに登録されていないと判別された場合、電子マネーサーバ13は、受信した個人公開鍵Pk2Aを用いて取引認証子{Pk1A(T150+取引情報+C99)}を取引情報とカードIDと端末IDに変換する。さらに、受信した端末公開鍵Tk2Bを用いて取引先認証子{Tk1B(T150+取引情報+C99)}を取引情報とカードIDと端末IDに変換し、これらが相互に一致するか否かを判別する。完全に一致した場合、電子マネーサーバ13は、カードID”C99”と個人公開鍵Pk2Aを認証付与要求と共に認証局11に送信する(L54)。

【0115】認証局11は、自分が記憶しているカードID及び個人公開鍵を参照し、受信したカードID”C99”と個人公開鍵Pk2Aがシステムに登録されているかをチェックし、登録済みであることを確認すると、センタ公開鍵Ck1を用いて認証情報{Ck1(C99+Pk2A)}を生成し、認証完了電文と共に電子マネーサーバ13に送信する(L55)。電子マネーサーバ13は、認証局11から認証情報{Ck1(C99+Pk2A)}を受信すると、受信した認証情報{Ck1(C99+Pk2A)}をセンター公開鍵Ck2を用いて、カードID”C99”と個人公開鍵Pk2Aに変換し、それらが正しいことを確認すると、残高テーブルのカードID”C99”

の残高が換金金額の5万円以上か否かを判別する。残高が5万円以上ならば、電子マネーサーバ13は、銀行センタ17へカードID" C99"と振替金額" 5万円"を含む振替依頼電文を送信する(L56)。

【0116】銀行センタ17は、電子マネーサーバ13から振替依頼電文を受信すると、口座テーブルを参照し、別段口座からカードID" C99"に対応する利用者Aの決済口座に5万円を振り替える。振替処理が完了すると、銀行センタ17は振替完了電文を電子マネーサーバ13に送信する(L57)。電子マネーサーバ13は、振替完了電文を受信すると、残高テーブルのカードID" C99"の残高から5万円を減算し、取引履歴を生成し、取引履歴テーブルに記憶する。次に、電子マネーサーバ13は、認証局11からの認証情報を取引履歴に付与し、換金完了電文と共に電子マネー端末15Bに送信する(L58)。

【0117】電子マネー端末15Bは、換金完了電文に応答し、受信した認証情報を $\{Ck1(C99 + Pk2A)\}$ をセンター公開鍵Ck2を用いて、カードID" C99"と個人公開鍵Pk2Aに変換し、その認証情報が正しいものであることを確認すると、受信した取引履歴を電子マネーカード19Aに送信する(L59)。電子マネーカード19AのIC部20は、受信した取引履歴に基づいて、自分が記憶する残高から5万円を減算する。さらに、電子マネー端末15Bは、受信した取引履歴を光記憶部21の最終取引ポインタが指示するアドレスの次のアドレスに追記し、最終取引ポインタと及び送信済みポインタの値を更新する。

【0118】このようにして、利用者は自己の電子マネーカード19に蓄積している電子マネーを換金し、自己の決済口座に振り込むことができる。

【0119】以上説明したように、この電子マネーシステムにより、電子マネーを電子マネーカードにチャージし、換金し、譲渡し、支払いに使用することができる。しかも、譲渡処理を行う際には、取引履歴情報に送金元の指紋データが付加されているので、取引履歴情報の改竄が困難であり、不正を予防できる。また、取引データの不整合が検出された場合には、各電子マネーカード19の光記憶部21に記録された取引履歴をたどることにより、不正の発生箇所を突き止めることができる。しかも、送金元と送金先の電子マネーカード19に記録される取引履歴情報が同一であるので、突き合わせが容易であり、追跡が容易である。

【0120】なお、取引履歴の構成要素は、上記に限定されず任意である。例えば、各取引履歴に、残高、固有の取引番号等を加えても良い。また、取引履歴から認証情報等を除いてもよい。

【0121】上記実施の形態では、電子マネーカード19の利用者の決済口座のリストを銀行センタ17に登録し、カードIDを決済口座の口座番号に変換したが、決

済口座の口座番号を電子マネーカード19のIC部20又は光記憶部21に登録しておき、電子マネーのチャージ、換金等の処理を行う際に、電子マネーカード19から口座番号を銀行センタ17に通知してもよい。

【0122】上記実施の形態では、個人認証情報を生成、確認するために署名鍵Skと検査鍵Ekを用いたが、センタ秘密鍵Ck1とセンタ公開鍵Ck2を用いてもよい。

【0123】ワイドエリアのネットワーク(例えば、インターネット等)のネットワーク上でこの電子マネーシステムを構築する場合は、認証局11と電子マネーサーバ13をそれぞれ設けることが望ましいが、クローズドループ型のローカルネットワークでは、認証局11と電子マネーサーバ13を、1つのサーバとして実現してもよい。

【0124】また、この電子マネーシステムは、図18に示すように、認証局11を除いた構成にしてもよい。この場合の各処理の概要を図19～図23に示す。これらの処理は、認証に関する処理がなくなった点を除けば、実施の形態の動作と同一である。このような構成によれば、システム全体において処理速度が向上する。

【0125】上記実施の形態では、譲渡処理をオンライン処理で行ったが、オフライン処理で行うことも可能である。オフライン処理で譲渡処理を行う場合の処理手順の例を図24を参照して説明する。なお、電子マネーを譲渡(送金)する側を電子マネーカード19Aとし、譲渡を受ける(受金)側を電子マネーカード19Bとする。

【0126】まず、図8に示す画面表示に従って、表示部32に表示される処理メニューから「3)電子マネーの譲渡」が選択され、送金側の電子マネーカード19Aが挿入口35A、に受信側の電子マネーカード19Bが挿入口35Bにそれぞれ挿入され、電子マネーカード19Aから電子マネーカード19Bへの譲渡金額が入力される。

【0127】電子マネー端末15は、この入力に応答して、電子マネーカード19Aと電子マネーカード19Bに、取引区分(19Aから19Bへの譲渡)と利用年月日と取引金額とから構成される取引情報と端末IDと、カードIDと個人公開鍵と残高の要求を示す要求信号をそれぞれ送信する(L41)。

【0128】電子マネーカード19Aは、要求信号に応答し、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Aを用いて、端末IDと取引情報と自己のカードIDに対する取引認証子 $\{Pk1A(\text{端末ID} + \text{取引情報} + 19A\text{のカードID})\}$ を作成する。電子マネーカード19Aは、作成した取引認証子とカードIDと個人公開鍵Pk2Aと指紋データと残高を電子マネー端末15に送信する(L42)。

【0129】また電子マネーカード19Bは、端末ID

及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Bを用いて、端末IDと取引情報と自己のカードIDに対する取引認証子〔Pk1B(端末ID+取引情報+19BのカードID)〕を作成する。電子マネーカード19Bは、作成した取引先認証子とカードIDと個人公開鍵Pk2Bとを電子マネー端末15に送信する(L42)。

【0130】電子マネー端末15は、電子マネーカード19Aの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末15に送信する。電子マネー端末15は、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【0131】残高が指示された譲渡金額以上の場合、電子マネー端末15は、電子マネーカード19Aの個人公開鍵Pk2Aを用いて取引認証子〔Pk1A(端末ID+取引情報+19AのカードID)〕を端末IDと取引情報と電子マネーカード19AのカードIDとに変換する。又、電子マネーカード19Bの個人公開鍵Pk2Bを用いて取引認証子〔Pk1B(端末ID+取引情報+19BのカードID)〕を端末IDと取引情報とカードIDとに変換する。次に、変換した内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から変換された取引情報及び端末IDが一致しており、取引認証子から変換されたカードIDが譲渡元の電子マネーカード19AのカードIDに一致し、取引先認証子から変換したカードIDが譲渡先の電子マネーカード19BのカードIDに一致することをチェックする。全て一致すると判別された場合、譲渡元(送金元)の電子マネーカード19Aの取引履歴と譲渡先(送金先)の電子マネーカード19Bの取引履歴を生成する。

【0132】電子マネー端末15は、生成した取引履歴を電子マネーカード19Aと電子マネーカード19Bへそれぞれ送信する(L47)。電子マネーカード19Aと19BのIC部20は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マネーカード19AのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード19BのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【0133】さらに、電子マネーカード19A、19BのIC部20は、それぞれ、最終取引ポインタの値を電子マネー端末15に送信する。電子マネー端末15は、電子マネーカード19Aと19Bの光記憶部21の、最終取引ポインタの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポインタを、追記された取引履歴を示すように更新する。ただし、送信済みポインタは更新しない。

【0134】このような譲渡処理を行った場合、その後のオンライン処理の際に、上述の突き合わせ処理を行う。

【0135】また、上述の支払処理では、電子マネーカードと電子マネー端末の間でオフラインで処理を行ったが、顧客の電子マネーカード19と店舗の電子マネーカード19との間での、売り上げ金額相当の金額の譲渡として支払いを処理することも可能である。この場合、例えば、図4(B)に示す電子マネー端末15は、顧客の電子マネーカード19を挿入するためのカード挿入口と、店舗の電子マネーカード19を挿入するためのカード挿入口を備える。店舗用カード挿入口には、開店時等に、店舗の電子マネーカード19を挿入しておく。

【0136】売上計算が終了すると、電子マネー端末15B(例えばPOS端末)は表示部32に売り上げ金額と支払い方法を問い合わせるメッセージを表示する。このメッセージに応じて、電子マネーによる支払いを選択し、顧客の電子マネーカード19Aを挿入口に挿入すると、電子マネー端末15は、取引区分と取引年月日と取引金額(支払金額)とから構成される取引情報と、端末IDと、カードIDと個人公開鍵と残高の送信を要求する要求信号を顧客の電子マネーカード19と店舗の電子マネーカード19に送信する(L21)。以後の処理は、上述のオンラインでの譲渡処理と同一である。

【0137】このような支払い処理によれば、支払い時の取引履歴に支払者の指紋データが含まれることになり、さらに、オンライン取引になるため、支払いの信頼性と追尾性が向上する。

【0138】なお、上述のオフラインでの譲渡処理を採用してもよい。

【0139】また、セキュリティを高めるため、例えば、電子マネー端末15の操作者の正当性を操作者の身体的特徴に基づいて判別してもよい。例えば、電子マネーカード19のIC部20の記憶回路に所持者の指紋データを配置しておき、電子マネー端末15の操作者の指紋をスキャンし、これらが一致する場合にのみ、以後の電子マネー取引処理を実行しても良い。この場合、電子マネー端末15には、図25に示すような指紋読取装置41が配置される。指紋読取装置41は、指紋をスキャンするための読取窓41Aと指を案内するためのガイド41Bを備える。

【0140】指紋読取装置41は、図26に示すように、読取窓41A内の画像(指紋の画像)をスキャンし、画像データを取得する画像取得部51と、画像取得部51で取得した画像データ(の波形)をフーリエ変換するフーリエ変換部52と、フーリエ変換部52で取得されたフーリエ級数の位相情報のみを抽出する位相情報抽出部53と、IC部20から読み出した位相情報と位相情報抽出部53で生成された位相情報を合成する位相合成部54と、合成部54で合成された位相情報をフーリエ変換して相関強度を得るフーリエ変換部55と、フーリエ変換部55で得られた相関強度と閾値を比較し、操作者が正当者であるか否かを判別する判別部56とよ

り構成される。

【0141】このような構成において、例えば、処理メニューの中から処理を選択し、電子マネーカードを挿入すると、電子マネー端末15で、図27に示すように、指紋読取装置41上に指を置く旨のメッセージを表示する。操作者がメッセージに従って指紋読取装置41上に指を置くと、指紋読取装置41の画像取得部51は、読取窓41A内の指紋をスキャンし、その画像を取り込む。フーリエ変換部52は、読み取られた画像をフーリエ変換し、位相情報抽出部53が位相情報を取り込む。

【0142】続いて、位相合成部54は、IC部20に登録されている位相情報を読み出し、位相情報抽出部から抽出された位相情報を合成し、さらに、フーリエ変換部55は合成データをフーリエ変換し、相関強度を求める。

【0143】判定部56は、相関強度が一定値以上の場合に、予めIC部20に登録されている指紋と読み取った指紋が類似し、操作者が電子マネーカード19の正当な保持者であると判別し、選択した処理に対応する以後の処理を可能とするように制御する。相関強度が一定値未満の場合、予めIC部20に登録されている指紋と読み取った指紋が類似しないと判断し、表示部32に指紋照合が一致しないため、以後の操作できない旨を表示し、電子マネーカード19を排出する。

【0144】このような構成によれば、操作者の身体的特徴に基づいて、操作者が正当な者か否かを判別し、電子マネーの取引を許可するか否かを判別することができる。従って、電子マネーの不正使用を有效地に防止できる。

【0145】なお、指紋の類似度を判別する手法及び回路は図26に示す回路及び方法に限定されず、他の手法を使用してもよい。

【0146】また、上記実施の形態においては、指紋の画像をフーリエ変換し、位相情報を抽出したものを指紋データとしてIC部20に格納したが、指紋を他の形式で変換して指紋データとしてもよい。例えば、指紋の画像の特定の位置のオン・オフを指紋データとしてもよい。

【0147】また、指紋データに限定されず、声紋、顔のパターン、網膜パターン等の個人の身体的特徴を表す個人特定情報を指紋データの代わりに或いは指紋データと組み合わせて使用してもよい。例えば、予め抽出しておいた声紋データをIC部20に格納しておき、電子マネーの譲渡（移転）時に、この声紋データを履歴情報に含ませてもよい。また、電子マネー端末15にマイクロフォンを配置し、マイクロフォンで取得した音声の特徴データを抽出し、IC部20に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別し、システムの使用を許可してもよい。

【0148】また、顔のパターン、網膜パターン等を使用する場合には、顔、網膜パターンの特徴データをIC部20に格納し、電子マネー端末15にカメラを配置し、カメラで取得した、画像の特徴データを抽出し、IC部20に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【0149】なお、予め抽出された特徴データは、IC部20に格納されてもよく、光記録部21に格納されて10も良い。

【0150】さらに、電子マネーカードに予め登録しておいて個人特定情報ではなく、指紋読取装置、マイクロフォン、カメラなどを介してリアルタイムで抽出した個人特定情報を、取引履歴情報に含ませても良い。

【0151】なお、電子マネーカード19の形状はカード型に限定されず任意である。

【0152】電子マネーを扱うシステムでは、例えば、利用者のカードID等の情報を入手して、そのカードIDの所有者になりすまして認証を得ようとする不正行為が考えられる。このような不正行為を防ぐために、通信電文等を例えばRSA方式等の暗号方式を用いて暗号化することにより、そのセキュリティを高めることができる。この場合、例えば、認証局11は、センタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、記憶する。認証局11は、電子マネーサーバ13にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ10内で共有化する。また、認証局11は、センタ公開鍵Ck2を各電子マネー端末15及び電子マネーカード19等に電子マネーサーバ13を介して予め配布する。

【0153】各電子マネーカード19及び電子マネー端末15は、センタ公開鍵Ck2を用いて各自の情報（電子マネーカード19ならばカードID及び個人公開鍵、電子マネー端末15ならばチャージ要求、種々の電文等）を暗号化し、電子マネーサーバ13に送信する。電子マネーサーバ13がセンタ秘密鍵Ck1を用いてそれらの情報を復号化し、処理する。電子マネーサーバ13は、電子マネーカード19から送られてきた個人公開鍵を用いて取引履歴を暗号化し、電子マネー端末15を介して電子マネーカード19に送信する。

【0154】このような手法を用いることにより、電子マネーカード19及び電子マネー端末15からの情報は、センタ10内の電子マネーサーバ13及び認証局11しか復号化することができず、又、電子マネーサーバ13からの取引履歴は、電子マネー端末15で参照されることなく、電子マネーカード19に送信され、復号化される。更に、秘密鍵・公開鍵を定期的に変更することにより、よりセキュリティを高めることができる。

【0155】なお、認証局11は、センタ秘密鍵Ck1及び公開鍵Ck2を定期的又は不定期に変更し、センタ公開鍵Ck2を電子マネー端末15へ、センタ秘密鍵Ck1を電50

子マネーサーバ13へ、それぞれ送信する。センタ秘密鍵Ck1及びセンタ公開鍵Ck2を変更した後、電子マネー端末15に電子マネーカード19が挿入されたとき、電子マネー端末15は、新たなセンタ公開鍵Ck2を電子マネーカード19に通知する。

【0156】また、暗号化の方式は、公開鍵方式に限定されず、共通鍵方式を用いてもよい。この場合、セキュリティの面から電子マネーカード19の耐タンパ性を強化することが望ましい。

【0157】また、このシステムで取引が行われる度に、新たな暗号化のキー（秘密鍵と公開鍵の対、共通鍵等）を発行し、電子マネーカードに通知して、通知されたキーを用いて暗号化・復号化を行ってもよい。

【0158】さらに、キーを乱数に基づいて発生してもよい。このようなシステムによれば、次に発行されるキーの予測がつかず、情報の漏洩を防止できる。過去に発行されたキーと新たに発行されたキーを組み合わせて暗号化及び復号化用のキーとして使用してもよい。例えば、今回のキーK_tと前回のキーK_{t-1}を組み合わせて{K_t+K_{t-1}}をキーとして用いて各種情報を暗号化し、さらに、復号化してもよい。

【0159】また、上記実施の形態では、認証局11に本システムにおいて使用可能な電子マネーカード19のカードID及び個人公開鍵を利用者をチェックするために予め登録しておき、さらに各電子マネーカード19に個人認証情報を付与するようにしているため、秘密鍵、暗号鍵を勝手に生成し、記憶した偽造カードによる不正を防ぐことができる。

【0160】電子マネーシステムにおいては、電子マネーカード19自体の完全なコピーを作成し、不正使用することが考えられる。この種の不正使用を防止するためには、電子マネーサーバ13で、取引毎に固有の番号を電子マネーカード19に付与し、オンライン取引開始時に、電子マネーカード19からこの固有番号を電子マネーサーバ13に送信し、電子マネーサーバに登録されているその電子マネーカード19の固有番号に一致することを確認してから取引を行い、取引終了時等に、新たな固有番号を発生して電子マネーカード19と電子マネーサーバ13に登録するよう構成すればよい。この構成によれば、取引の度に、固有番号が更新されるため、電子マネーカード19のコピーを作成しても、1回取引を行うと、使用した1枚以外は固有番号が電子マネーサーバ13に登録されているものと異なってしまうため、使用できなくなる。従って、電子マネーカード19のコピーによる不正使用を防止できる。

【0161】なお、上記説明では、カードへの電子マネーのチャージ処理に際して、チャージ金額相当の現金を利用者の口座からシステムの決済口座に移動させて、該チャージ金額を支払うようにしているが、例えばクレジットによる支払としてもよい。この場合、例えば、サー

バが、チャージ要求の受信に応じて、該要求が示すチャージ金額、利用者の口座等の情報を貸付情報として一定期間記憶しておき、所定のタイミングで、利用者の口座から引き落とす。

【0162】なお、この発明の電子マネー端末は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、CD-ROM等）から該プログラムをインストールすることにより、上述の処理を実行する電子マネー端末を構成することができる。

【0163】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的に且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OSの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0164】

【発明の効果】以上説明したように、本発明によれば、電子マネーカードに電子マネーをチャージし、チャージした電子マネーを用いて種々の取引を行うことができる。しかも、取引履歴に指紋データ等の身体的特徴を示す特徴データを含ませているので、データの改竄等が困難である。また、この取引履歴を追記型記録部に記録することにより、この追記型記録部の記録内容を検証することにより、不正行為等を容易に検出することができる。さらに、センタのコンピュータにおいても取引履歴を記録することにより、不正行為をより確実に検出することができる。また、電子マネーの授受（送金）を指示する電文に個人特定情報を含ませ、これを端末からコンピュータに送信することにより、コンピュータで個人特定情報を用いて電文の正当性をチェックすることができ、システムの信頼性を高めることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図2】（A）は、電子マネーサーバが記憶している残高テーブルの構造を示す図、（B）は、電子マネーサーバが記憶している事故カードリストの構造を示す図、（C）は、電子マネーサーバが記憶している事故端末リストの構造を示す図である。

【図3】電子マネーサーバが記憶している取引履歴テーブルの構造を示す図である。

【図4】（A）と（B）は、電子マネー端末の外観構成の例を示す図である。

【図5】銀行センタが記憶している口座テーブルの構造を示す図である。

- 【図6】電子マネーカードの構造を示す図である。
- 【図7】電子マネーチャージ処理の流れを説明するための図である。
- 【図8】電子マネー端末の表示例を示す図である。
- 【図9】電子マネー譲渡処理の流れを説明するための図である。
- 【図10】電子マネー譲渡処理の流れを説明するための図である。
- 【図11】(A)は、電子マネー譲渡処理時の譲渡元の電子マネーカードの取引履歴の例を示す図である。
- (B)は、電子マネー譲渡処理時の譲渡先の電子マネーカードの取引履歴の例を示す図である。
- 【図12】連続的に電子マネー譲渡処理を行った場合に、各電子マネーカードに格納される取引履歴の主要部の例を示す図である。
- 【図13】個人認証情報発行処理の流れを説明するための図である。
- 【図14】電子マネー支払い処理の流れを説明するための図である。
- 【図15】突き合わせ処理の流れを説明するための図である。
- 【図16】突き合わせ処理において未送信履歴の送信前と送信後のIC部と光記憶部と残高テーブルの状態を示す図である。
- 【図17】電子マネー換金処理の流れを説明するための図である。
- 【図18】認証局を含まない場合の電子マネーシステムの構成の一例を示す図である。
- 【図19】認証局を含まない場合の電子マネーチャージ処理の流れを説明するための図である。

10

20

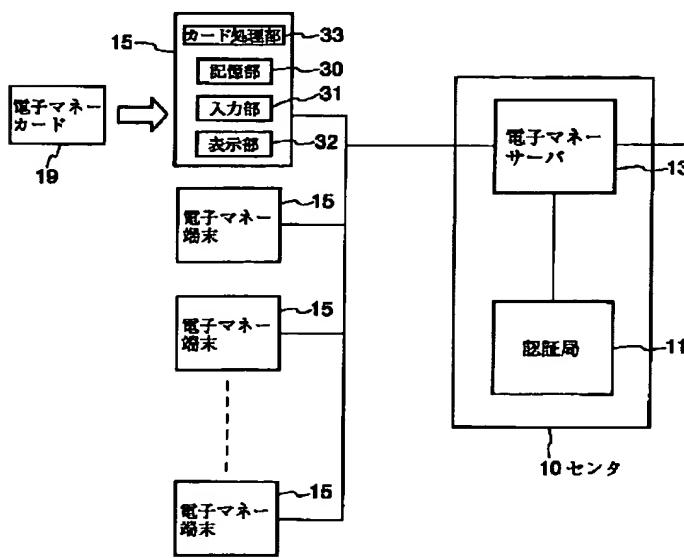
* 30

- * 【図20】認証局を含まない場合の電子マネー譲渡処理の流れを説明するための図である。
- 【図21】認証局を含まない場合の電子マネー支払い処理の流れを説明するための図である。
- 【図22】認証局を含まない場合の突き合わせ処理の流れを説明するための図である。
- 【図23】認証局を含まない場合の電子マネー換金処理の流れを説明するための図である。
- 【図24】オフラインでの、電子マネー譲渡処理の流れを説明するための図である。
- 【図25】指紋読み取り装置の例を示す図である。
- 【図26】指紋照合回路の構成例を示す図である。
- 【図27】指紋照合時の電子マネー端末の表示例を示す図である。

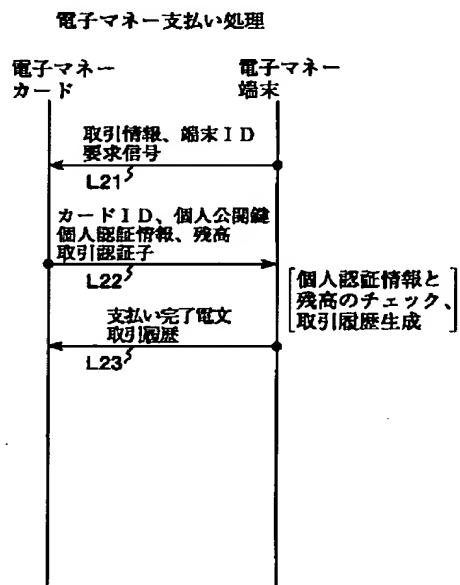
【符号の説明】

- 10 センタ
11 認証局
13 電子マネーサーバ
15 電子マネー端末
17 銀行センタ
19 電子マネーカード
20 IC部
21 光記憶部
30 記憶部
31 入力部
32 表示部
33 カード処理部
34 タッチパネル
35、35A、35B カード挿入口
* 36 金銭ドロア

【図1】



【図14】



【図2】

(A) 残高テーブル

カードID	残高
C001	50000
C003	10000
C005	5000
C010	30000
⋮	⋮
⋮	⋮

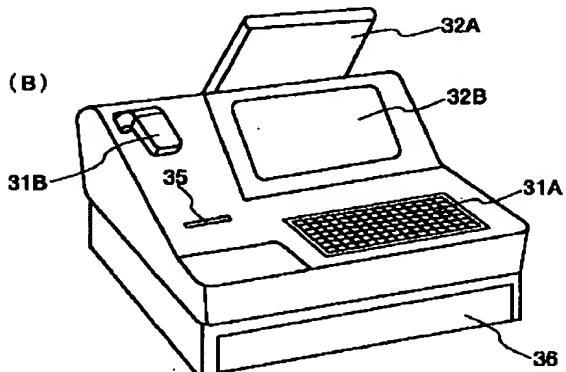
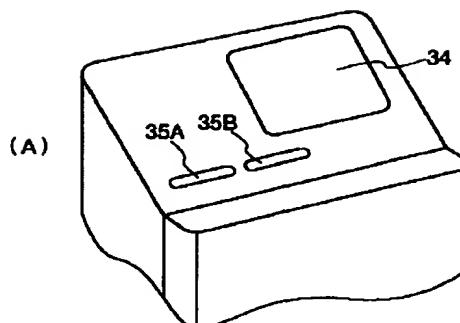
(B) 事故カードリスト
(使用不可の電子マネーカード
のカードIDリスト)

カードID (使用不可)
C010
C021
C038
C048
⋮

(C) 事故端末リスト
(使用不可の電子マネー端末
の端末IDのリスト)

端末ID
T145
T247
T255
T301
⋮
⋮
⋮

【図4】



【図3】

取引履歴テーブル

カードID: C99

利用区分	端末ID	利用年月日	入・出金情報			履歴	
			確認元指紋データ	確認元カードID	金額	取引履歴	取引先履歴
チャージ	T110	88/02/20			98251	xxxxxxxxxxxx	xxxxxxxxxxxx
購入	T150	88/04/01	Aの指紋データ	C09	80000	xxxxxxxxxxxx	xxxxxxxxxxxx
支払	T110	88/04/80			8812	xxxxxxxxxxxx	xxxxxxxxxxxx
換金	T117	88/05/01			612	xxxxxxxxxxxx	xxxxxxxxxxxx
購入	T150	88/05/07	Yの指紋データ	C09	909	xxxxxxxxxxxx	xxxxxxxxxxxx
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

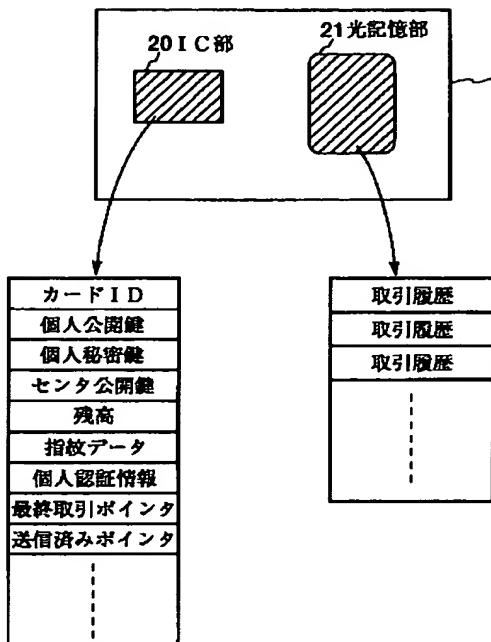
-----取引情報-----

【図5】

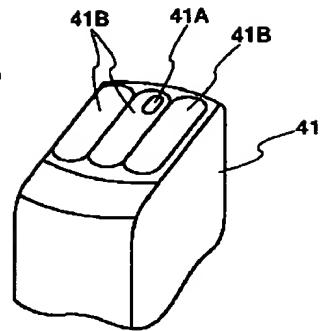
口座テーブル

カードID	口座番号
C01	10002221
C03	12341234
C05	53334442
:	:
C88	30000001
:	:
:	:

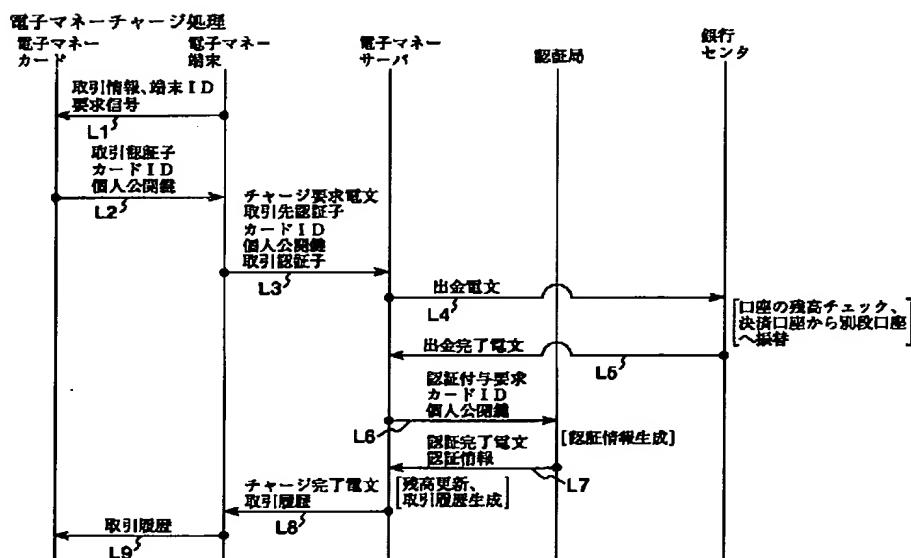
【図6】



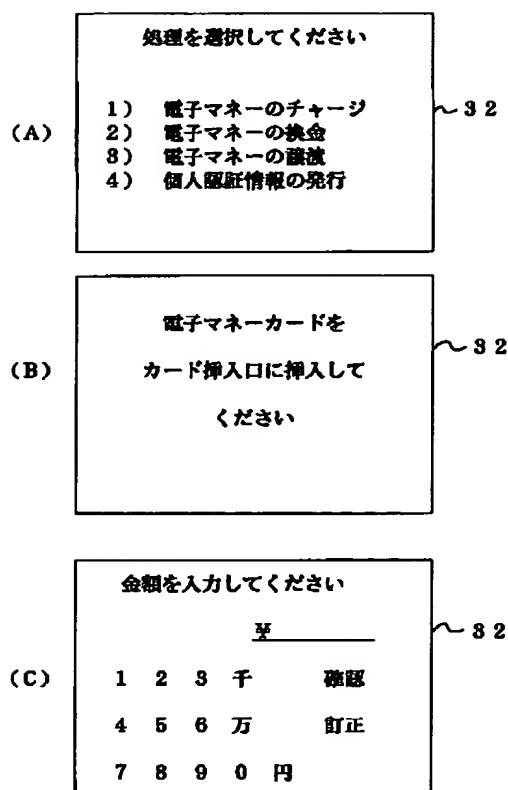
【図25】



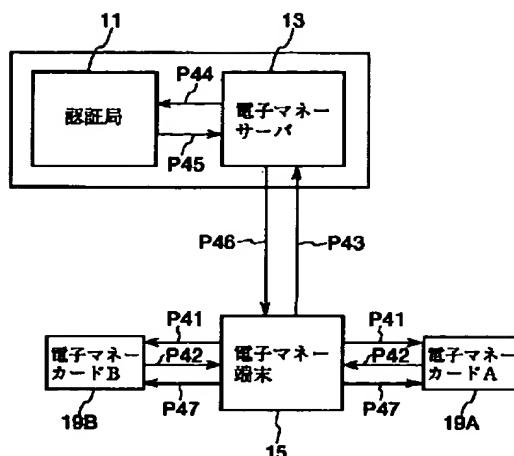
【図7】



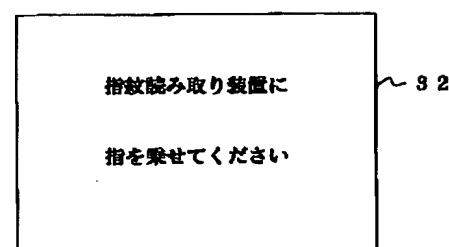
【図8】



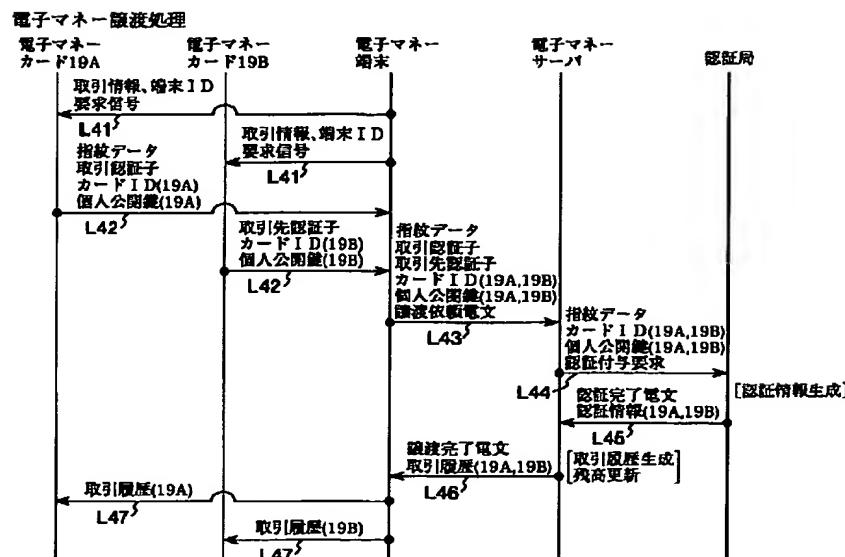
【図9】



【図27】



【図10】



【図11】

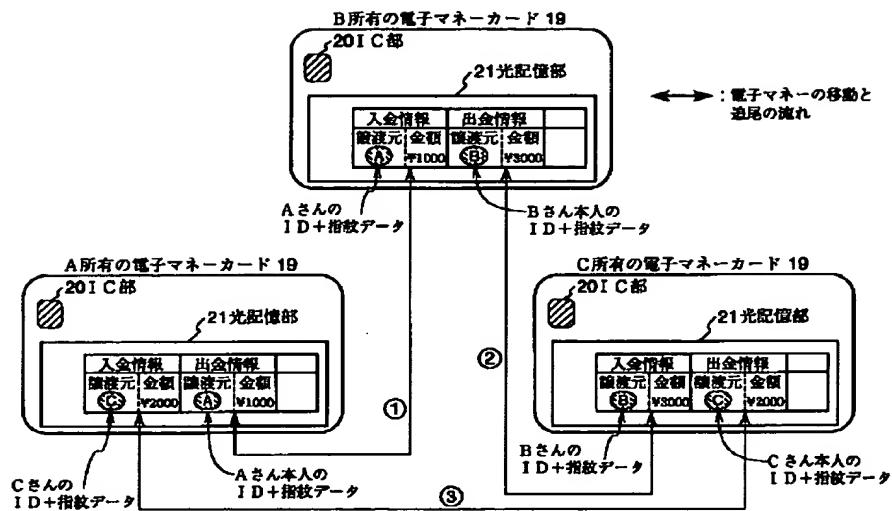
(A) 誰送元電子マネーカード19Aの取引履歴

利用区分	端末ID	利用年月日	出金情報			認証子
			誰送元指紋データ	誰送元カードID	金額	
誰送	T150	EE8/9/30	Aの指紋データ	C99	30000	PK1A (T150 + 取引情報 + C99) PK1B (T150 + 取引情報 + C05)

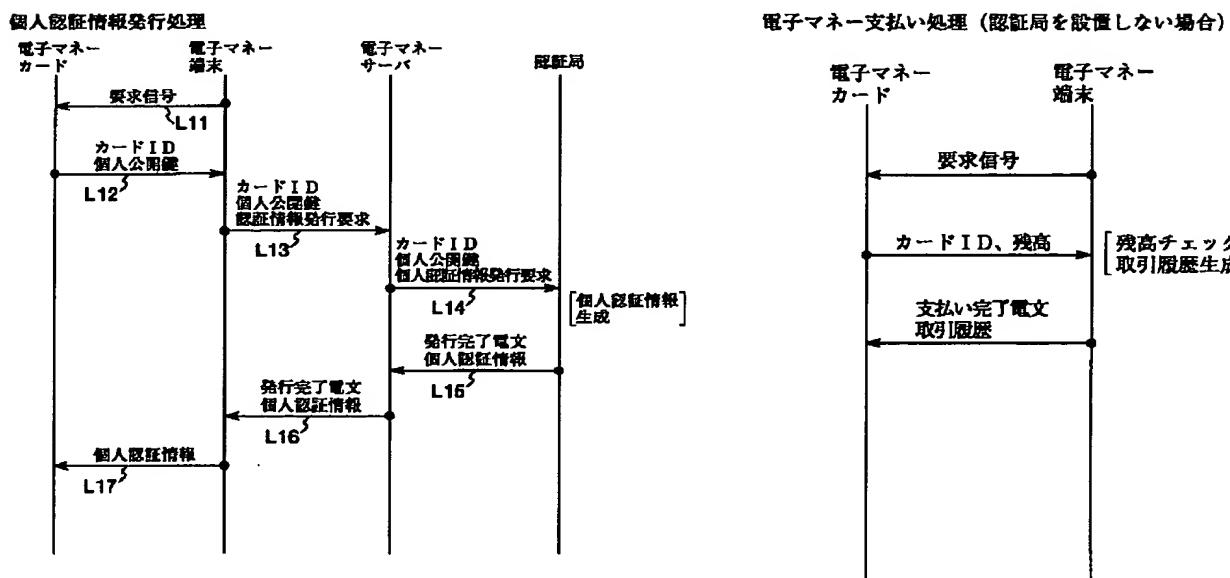
(B) 誰送先電子マネーカード19Bの取引履歴

利用区分	端末ID	利用年月日	入金情報			認証子
			誰送元指紋データ	誰送元カードID	金額	
誰送	T150	EE8/9/30	Aの指紋データ	C99	30000	PK1A (T150 + 取引情報 + C99) PK1B (T150 + 取引情報 + C05)

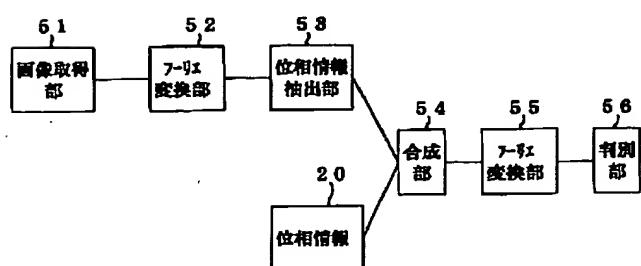
【図12】



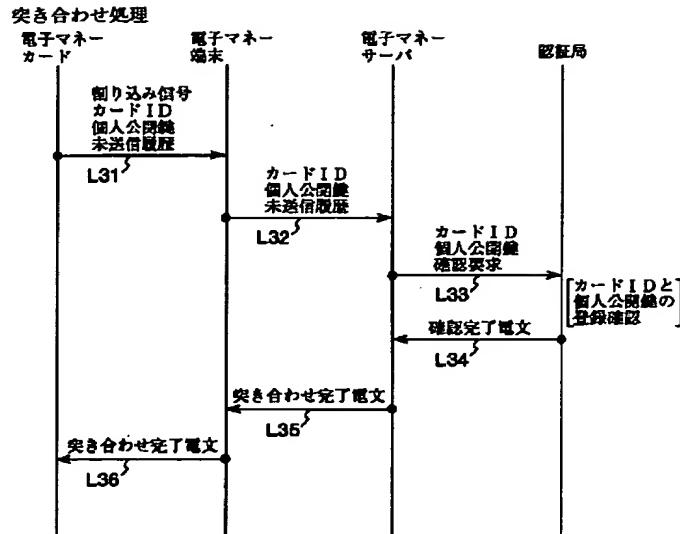
【図13】



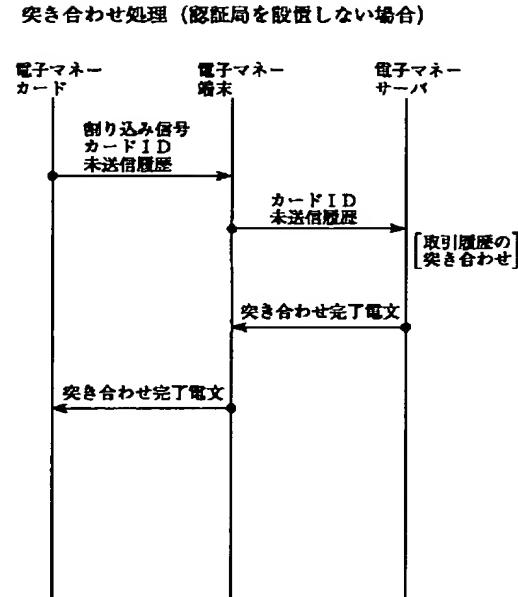
【図26】



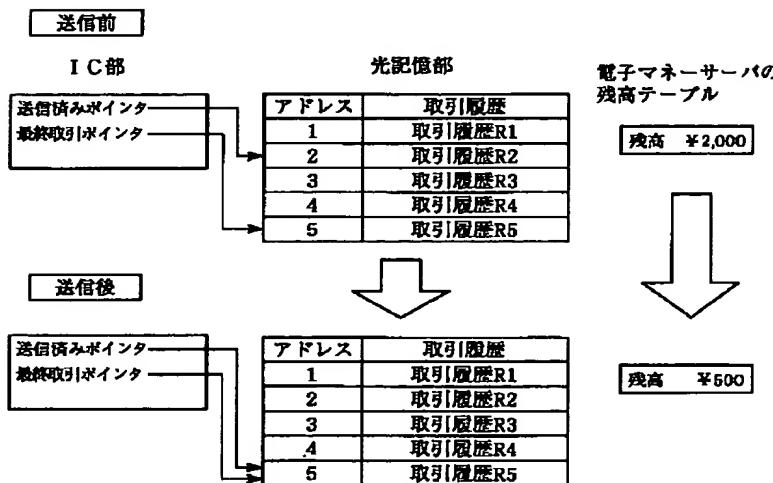
【图 15】



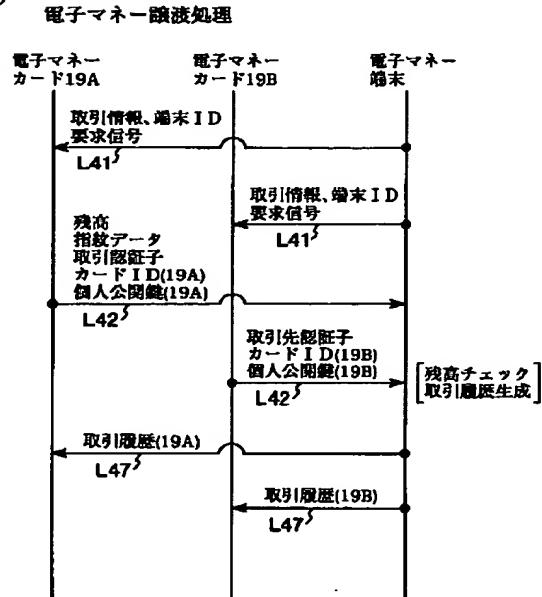
[図22]



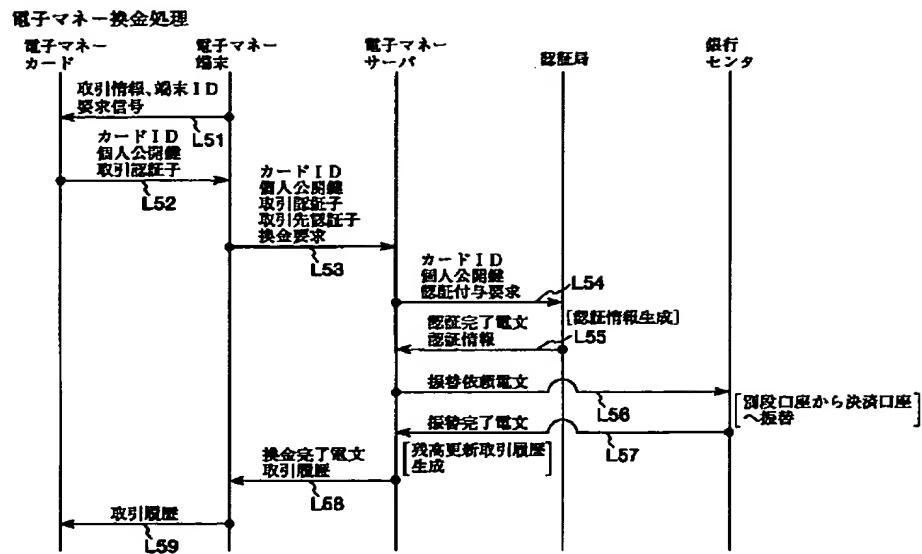
〔図16〕



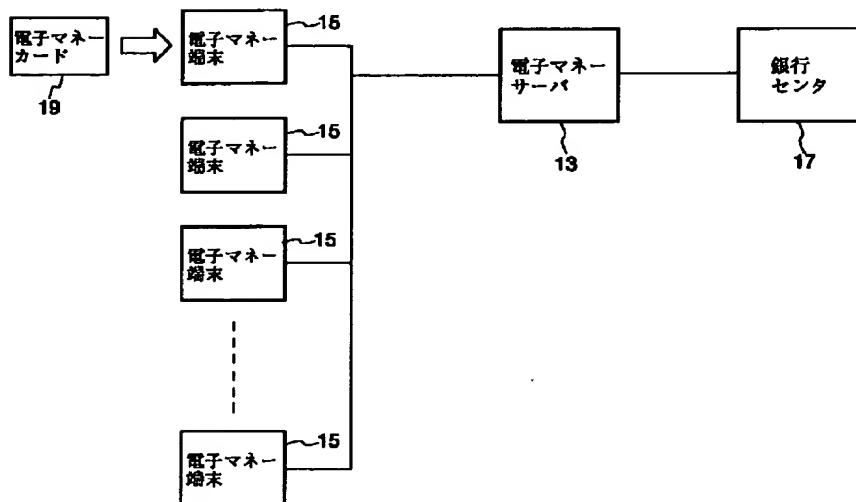
〔图24〕



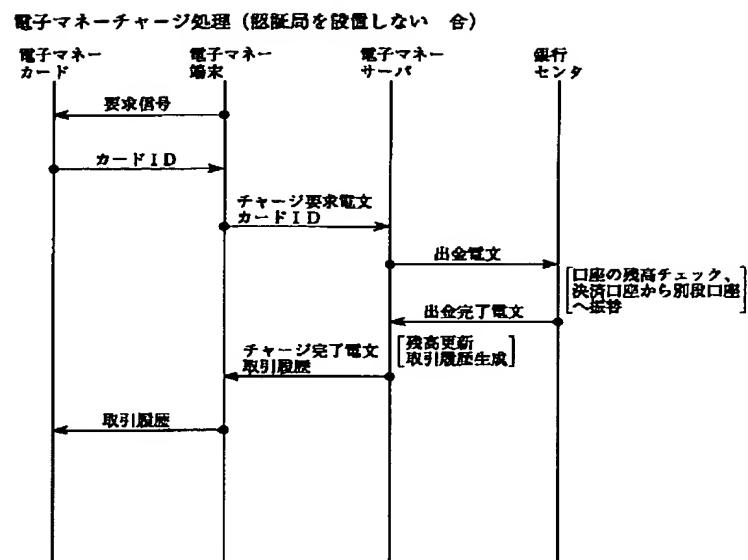
【図17】



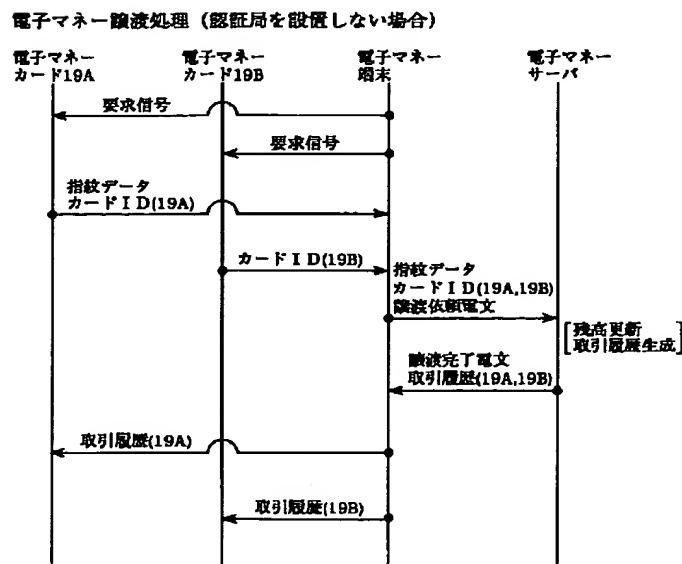
【図18】



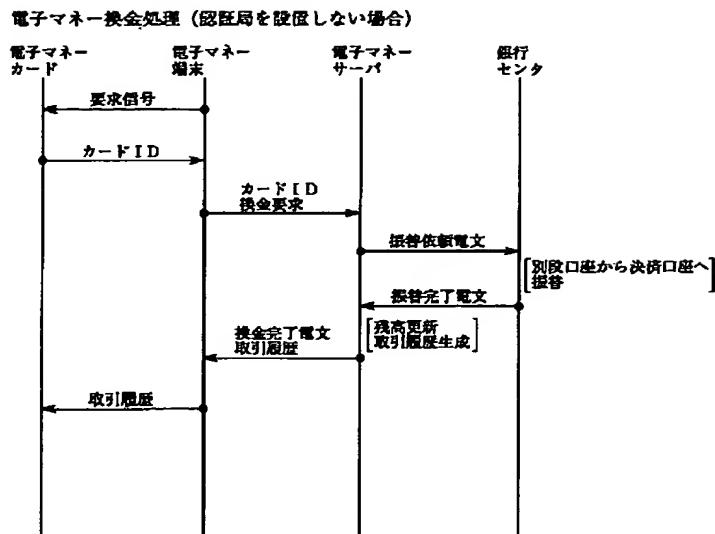
【図19】



【図20】



【図23】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

G 0 7 F 7/08

R

(72) 発明者 飯田 利英

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内